Telecom Signaling attacks on 3G and LTE networks

from SS7 to all-IP, all open

Philippe.Langlois@p1sec.com

P1 Security Inc.

v1.1

Telecom security intro

P1 Security
Priority One Security

- SIP, PBX, ...
- Periphery, customer side.
- Long gone world of Blue Box.
- Sometime hear about “Roaming frauds”.
- Rarely hear the Core Network horror stories.

Fugitive VOIP hacker cuffed in Mexico

More than 10 million minutes hijacked

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Security, 11th February 2009 22:33 GMT

Two charged with VoIP fraud

Hacking returns to phreaking roots

By **John Oates** • **Get more from this author**

Posted in Enterprise Security, 8th June 2006 09:51 GMT

Romanian Police Arrest 42 VoIP Hackers

December 20, 2010
By eSecurityPlanet Staff
Submit Feedback »
More by Author »

Police in Romania recently busted a hacking ring that was focused on stealing VoIP data from hacked servers.

"Agence France Presse reported on Tuesday that 42 people were arrested in the sting, breaking up a network that was headed by two Romanians and that had caused more than $13.5 million in losses to firms in the U.S., Britain, South Africa, Italy and Romania," writes threatpost's Paul Roberts.

Steve Jobs and Steve Wozniak in 1975 with a bluebox

http://www.p1security.com/

P1 Security
Priority One Security

Telecom frauds and attacks

UID	Issue	Risk	Cost
	Reverse Charge SMS Fraud	*Medium*	*High*
	Prepaid Abuse	*High*	*High*
	SS7 Entry Point Abuse	*Medium*	*High*
	Hostile SS7 Location Requests	*High*	*Low*
	Country-Wide Denial of Service	*High*	*High*
	User-Targeted Denial of Service	Medium	*Medium*

http://www.p1security.com/

P1 Security
Priority One Security

Telecom frauds and attacks

UID	Issue	Risk	Cost
	Femto-Cell Based Signaling Attacks	*High*	*Medium*
	Billing System Flooding for Prepaid Abuse	*Medium*	*High*
	SMSC Scanning, Discovery and Abuse	*High*	*Medium*
	SS7 MSU Bill Artificial Inflation	*Medium*	*Medium*
	VoIP Originated SS7 Injection	*Medium*	*High*
	Location Based Services Unauthorized Usage	Medium	*Medium*

http://www.p1security.com/

P1 Security
Priority One Security

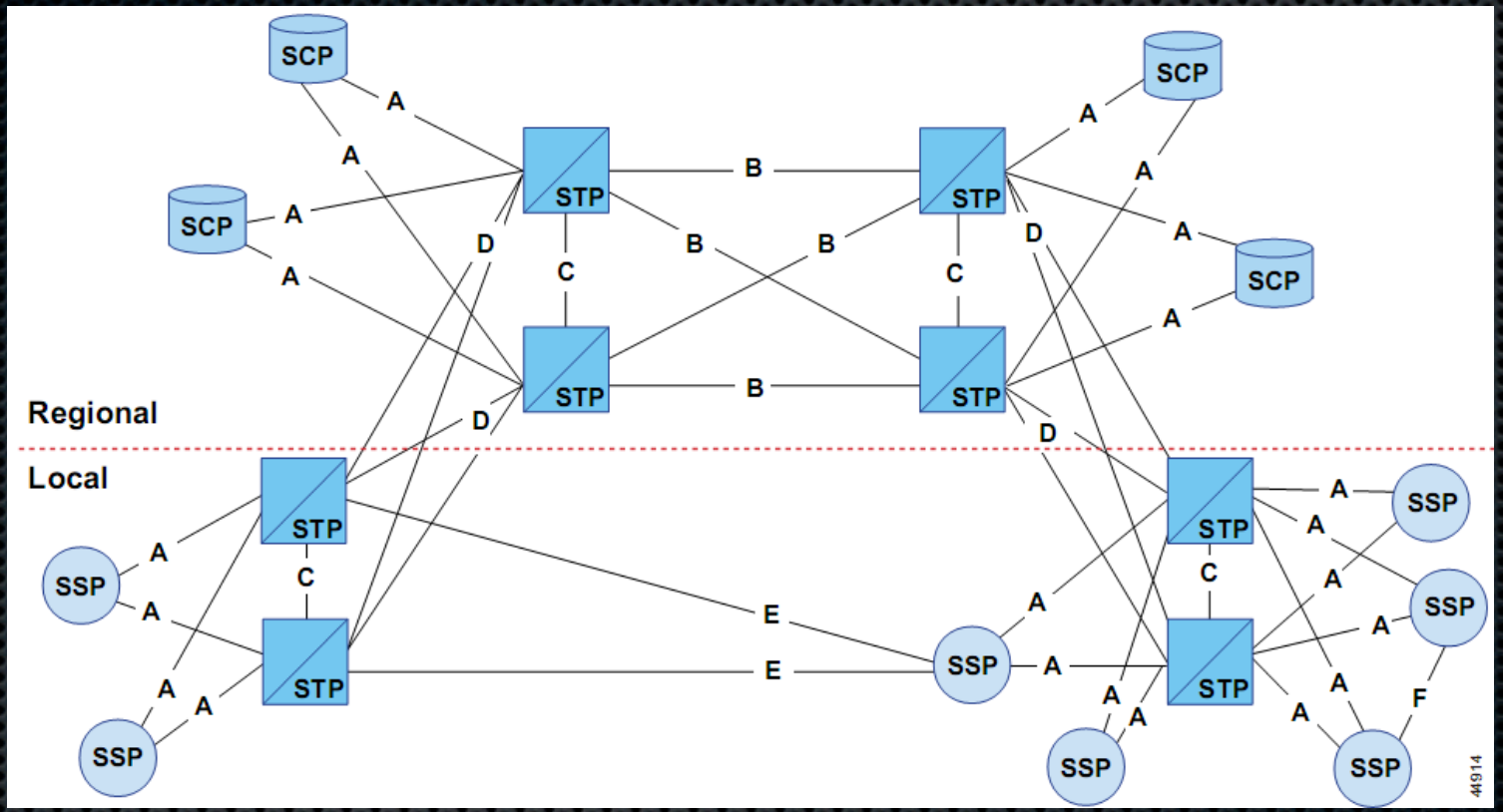
Telecom frauds and attacks

UID	Issue	Risk	Cost
	HLR Authentication Flooding	*High*	*High*
	VLR Stuffing	*High*	*High*
	Illegal Call Redirection	*Medium*	*High*
	Fixed Lines Capacity Denial of Service	*High*	*High*
	SMS to MSC Direct Addressing	*High*	*Medium*
	Region or Country Network Instability	*High*	*High*

http://www.p1security.com/

P1 Security
Priority One Security

Structure of operators: SS7

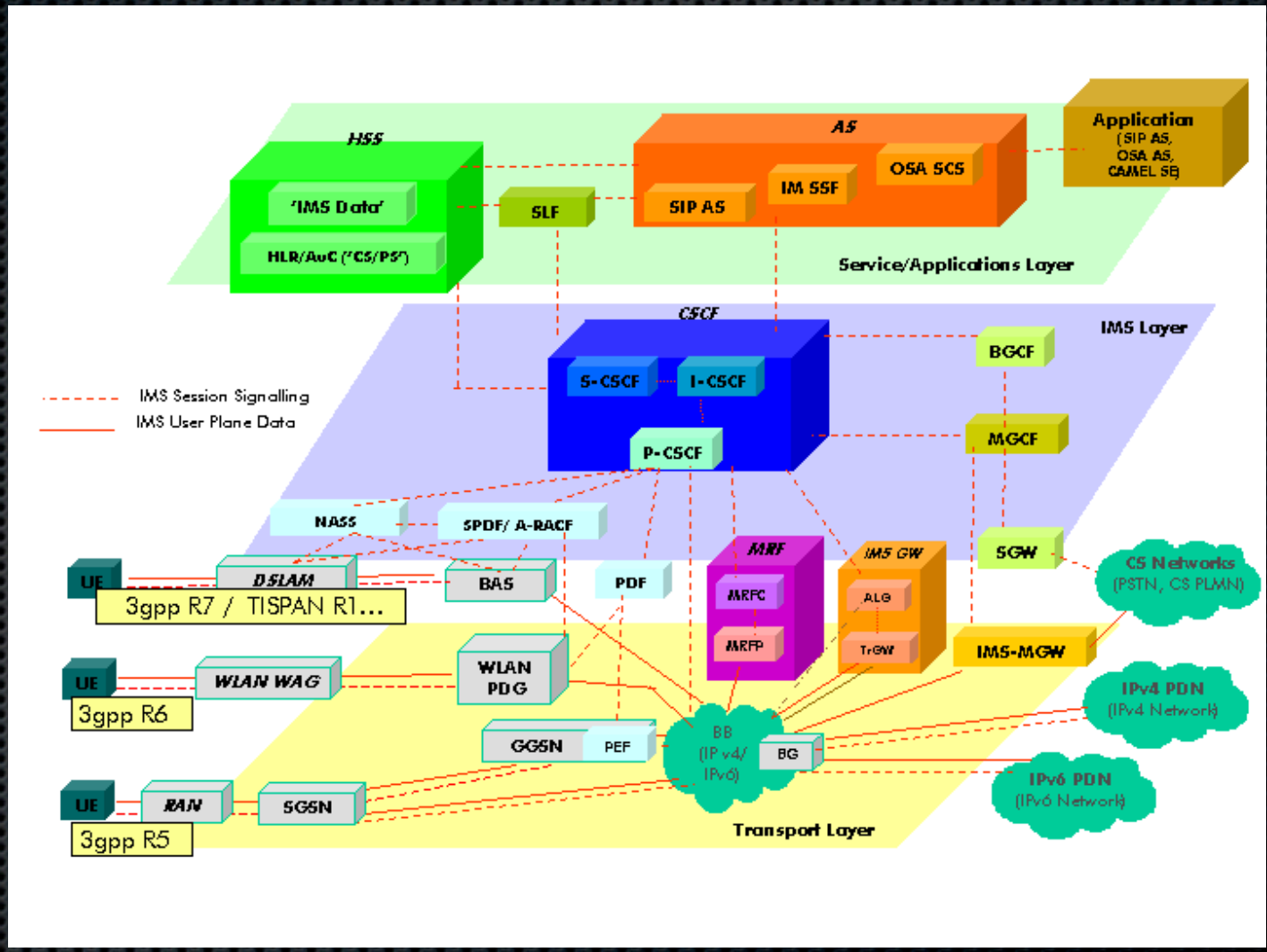


- SS7 basis for international interconnection & transit
- Called “Legacy”: Why it is not going away?
- “Walled garden” approach to security.

http://www.p1security.com/

NGN, IMS, 3G

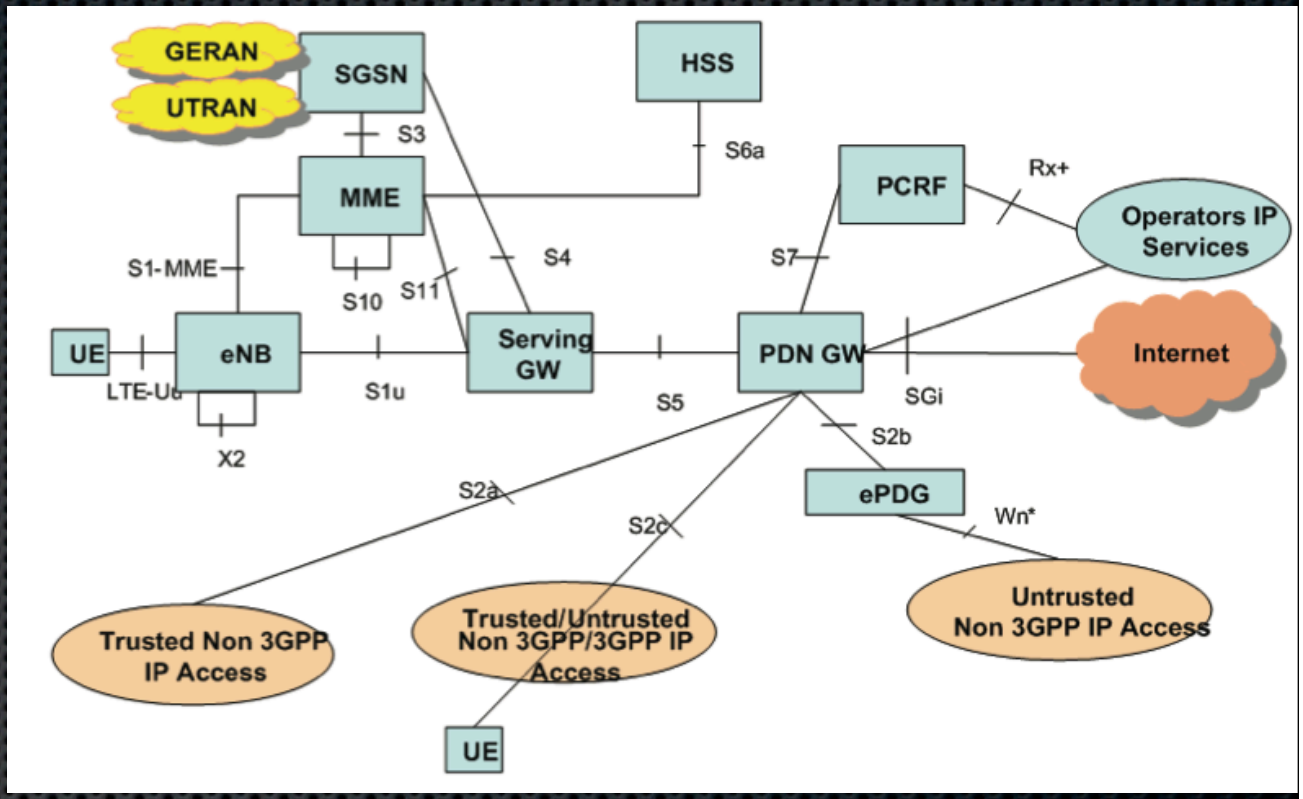
- IP friendly.
- More “IETF”
- Diameter
- Partly SIP-based
- SCTP appears
- Encapsulates SS7 over IP
- SIGTRAN



http://www.p1security.com/

LTE, LTE Advanced

- More “P2P”
- Even more IP
- SIGTRAN is simplified
- Simpler protocols (S1)
- eNB handover & communications
- Deeper integration, less layering & segmentation
- Addresses performances issues & bottlenecks



P1 Security
Priority One Security

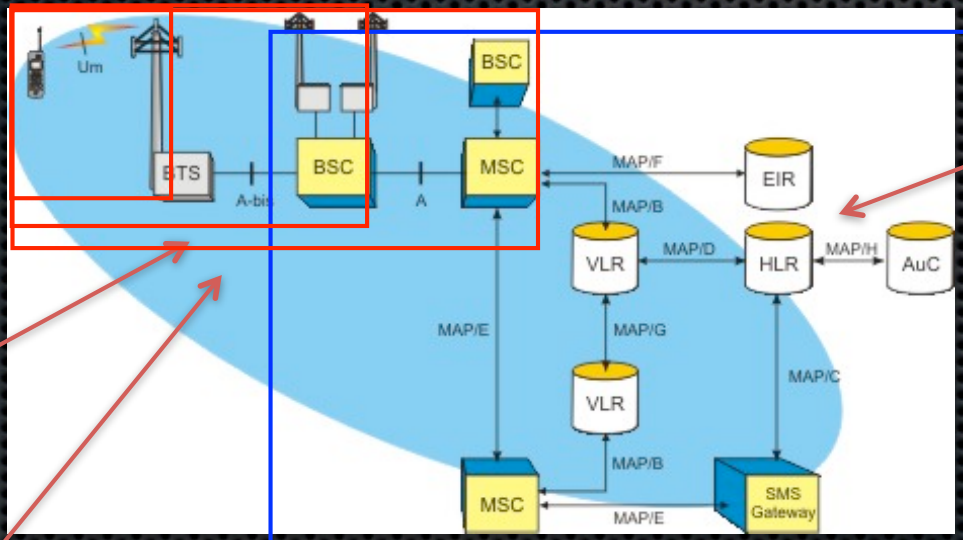
Current state of security research

ME vulnerability research (SMS o Death, OsmocomBB)

OpenBTS + crypto cracking (Karsten Nohl, ...), Baseband vulns (R.P. Weinman)

OpenBSC

FemtoCell hacking (THC, P1 Security, SEC-T, ...)



External APIs to HLR: location, IMSI. (Tobias Engel, ...)

Scanning and Attacking SS7 CN, SIGTRAN, IMS vulnerabilities, LTE scanning, ... (Philippe Langlois, P1 Security, Enno Rey)

SMS injection (TSTF, ...)

Nothing really new in IP domain?
WRONG:
Many things come from Telecom and IP merger & legacy obscurity.

P1 Security
Priority One Security

Attacking Telecom Networks

- Newbie question “How do you get access?”
- Steps
  1. Footprint
  2. Scan
  3. Exploit
  4. Detect & Protect
- No “recipe” as in IP world, each telecom environment is quite different (legacy sandwich)

1. Footprint (demo)

P1 Security
Priority One Security

Demo

http://www.p1security.com/

P1 Security
Priority One Security

2. Scan: PS entry points

- PS Domain is huge now
- Many common mistakes:
  - IP overlaps,
  - APN misconfiguration,
  - firewall issues,
  - IPv6 control
  - M2M specifics.

GTP entry points

P1 Security
Priority One Security

- GTP', GTP-C, GTP-U, v1 or v2
- UDP or SCTP based
- Many APNs (from 100-200 to 5000), many configurations, many networks with their corresponding GGSN.
- packet "slips" in M2M or public APNs
- GTP tunnel manipulation means traffic insertion at various point of the network (Core or Internet)

P1 Security
Priority One Security

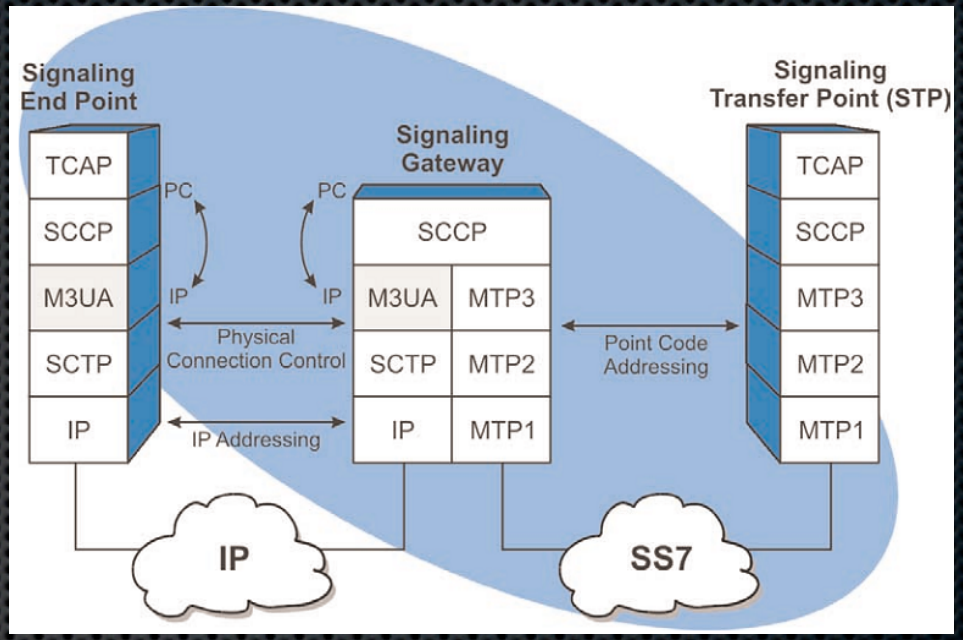
Scan Femto Cells entry points

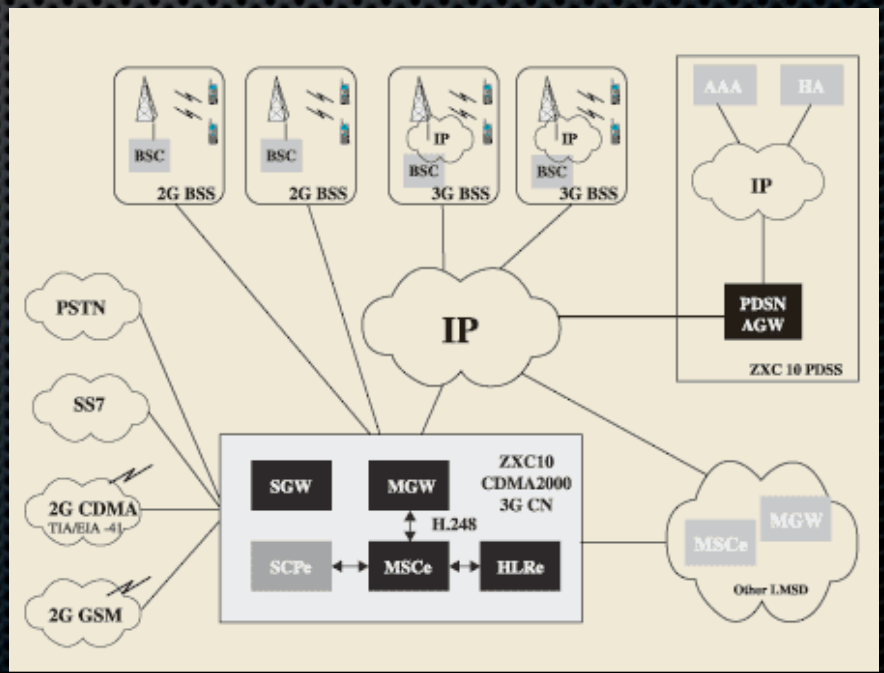
- Femto Cell security is improving
  - Better boot harden
  - IPsec tunnels
  - EAP-SIM protected
- But many compromise vectors still.
- Exposes directly signaling network (HNBAP), HLR/HSS (Diameter, ...), infrastructure network (routing, NTP, ...) to the user.

P1 Security
Priority One Security

Scan the Core Network

- Some Core Network start of migration since 2008 to IPv6
- SCTP based (RFC4960, Stream Control Transmission Protocol)
- Still SS7 encapsulated
- Implementations make scanning easy...

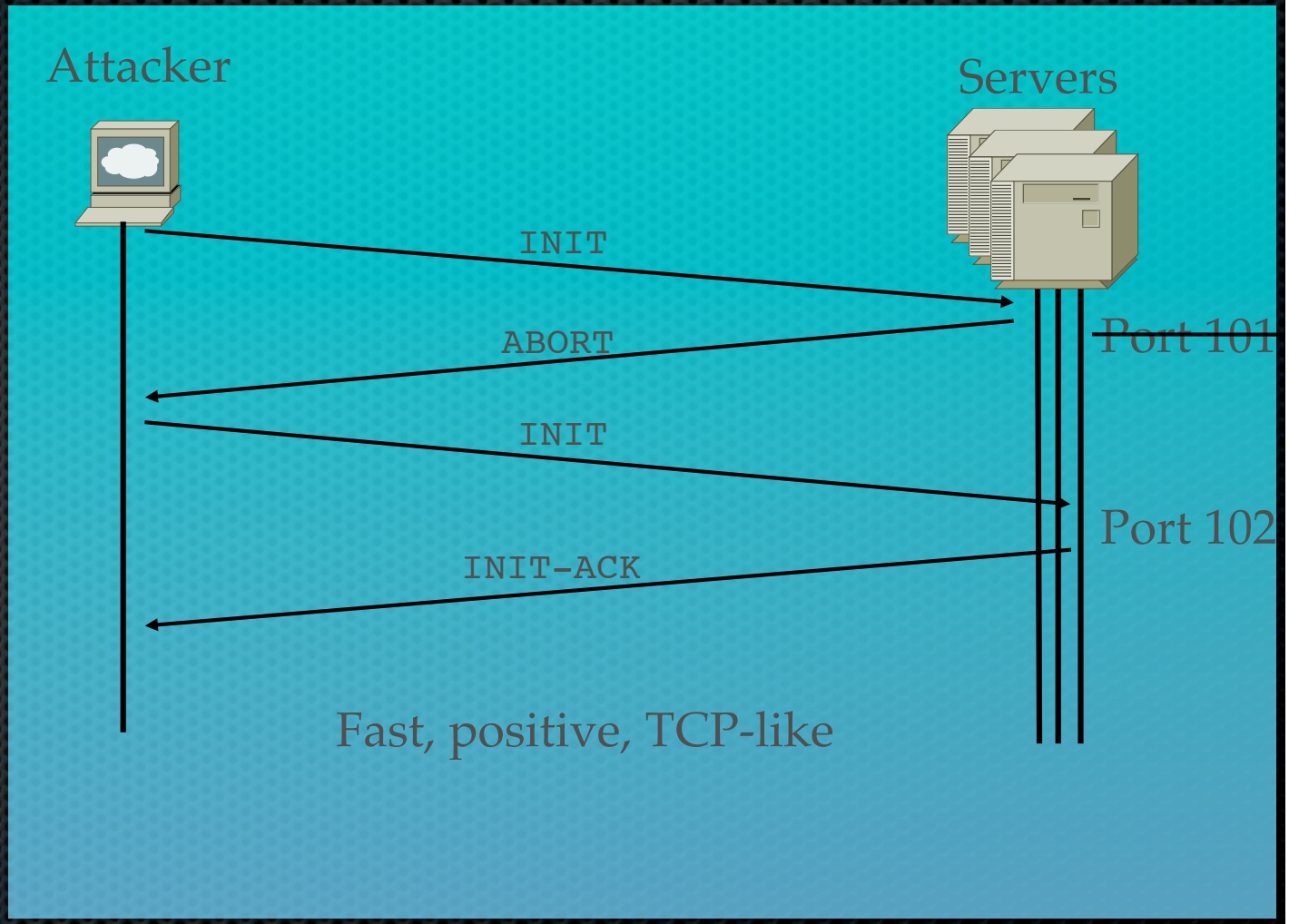




http://www.p1security.com/

SCTP scan

- Pioneered in SCTPscan, ported into nmap.
- Both don't work anymore (SCTP protocol evolved).
- Now in SCTPscan NG

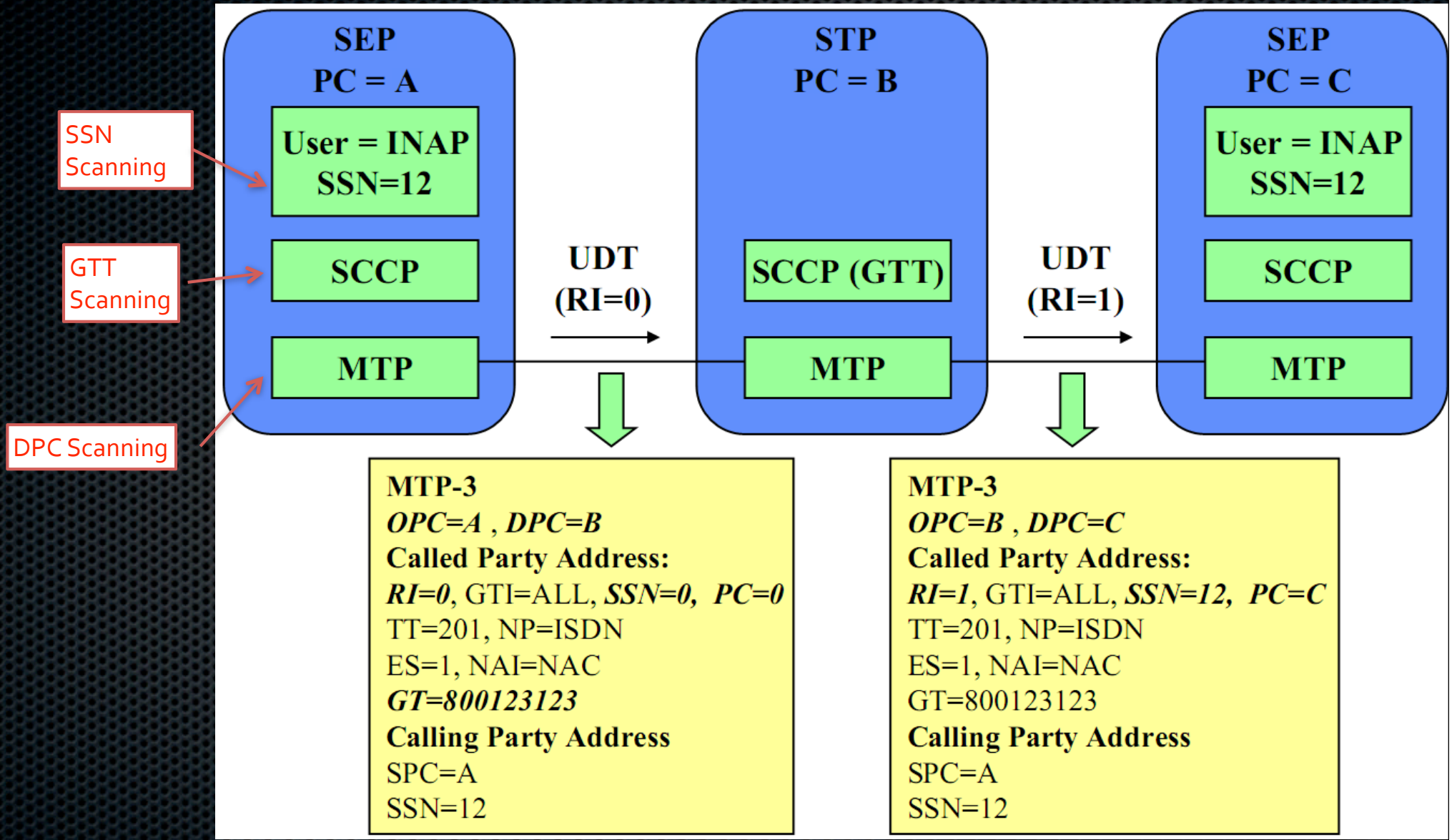


P1 Security
Priority One Security

CN Scan problems

- SCTP changed a lot, public tools don't work anymore. (Difficulty)
- IPv6 starts to be deployed, scan is completely possible but "regular consultants" don't know how to. (Size)
- CN Protocols are very complex (ASN.1 madness, Difficulty) cannot be tested by hand
- Signaling protocols address ranges makes then hard to assess by hand (Size)
- Size + Difficulty increase requires automation

Scan & Address spaces

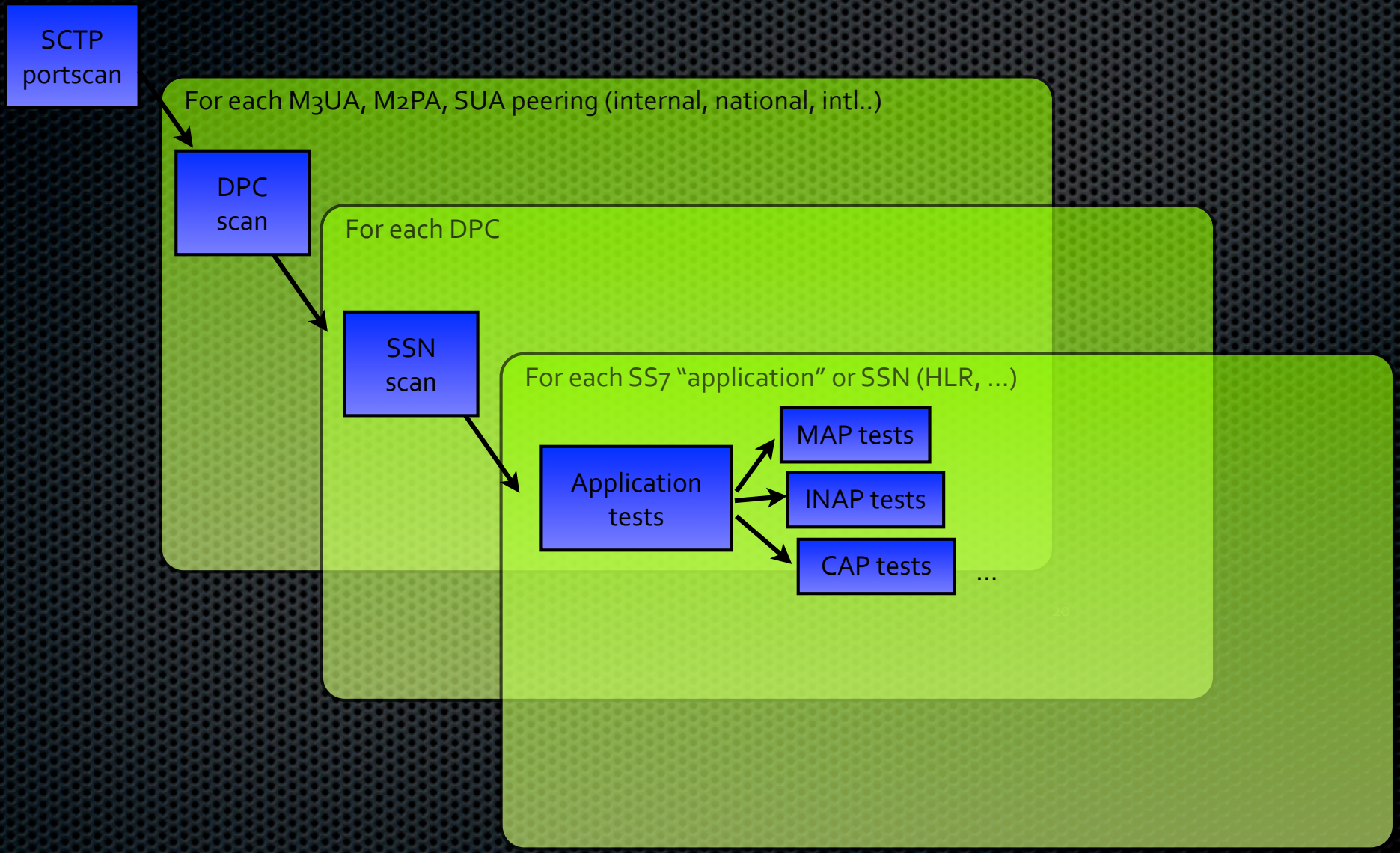


P1 Security
Priority One Security

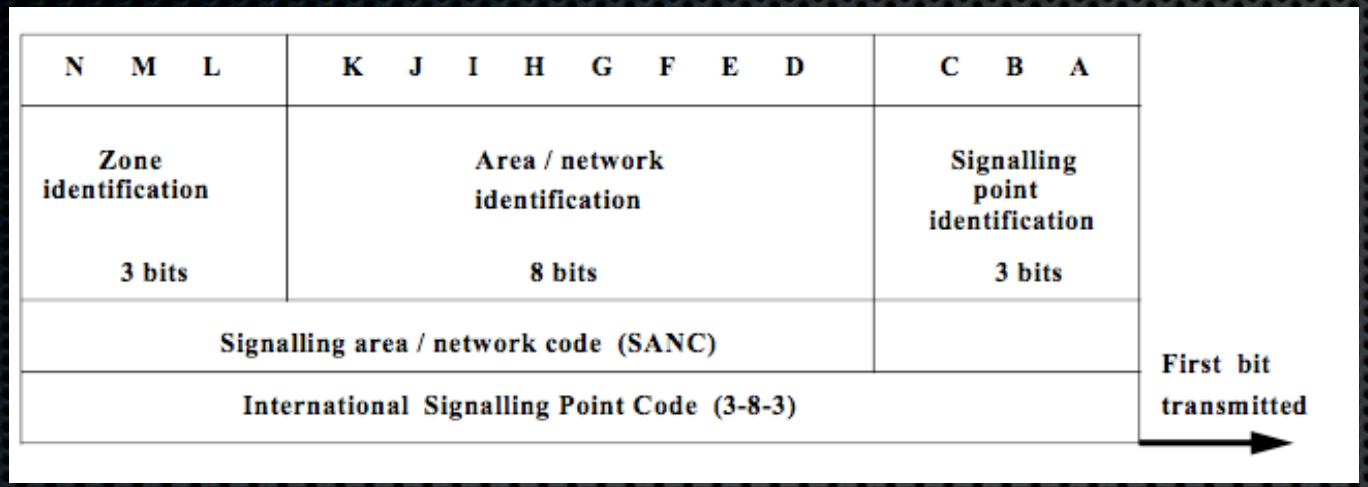
Scan IP vs. Telecom Signaling

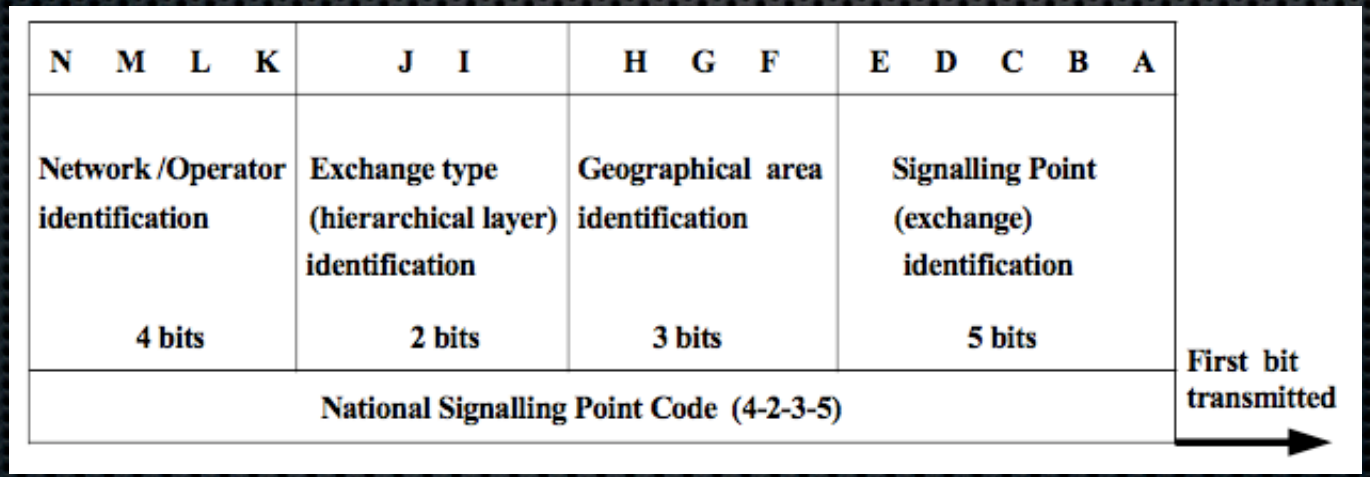
TCP/IP	SS7
IPsec endpoint scan, MPLS label scan, VLAN tag scan	SCTP endpoint scan
Arp or Ping scan	MTP3 or M3UA scanning
Ping scan using TCP SYN	SCCP DPC scanning
TCP SYN or UDP port/service scanning	SCCP SSN (SubSystem Number) scanning
Service-specific attacks and abuses (e.g. attacks over HTTP, SMB, RPC, ...)	Application (*AP) traffic injection (e.g. MAP, INAP, CAP, OMAP...)

SIGTRAN Audit Strategies



National and International SPCs



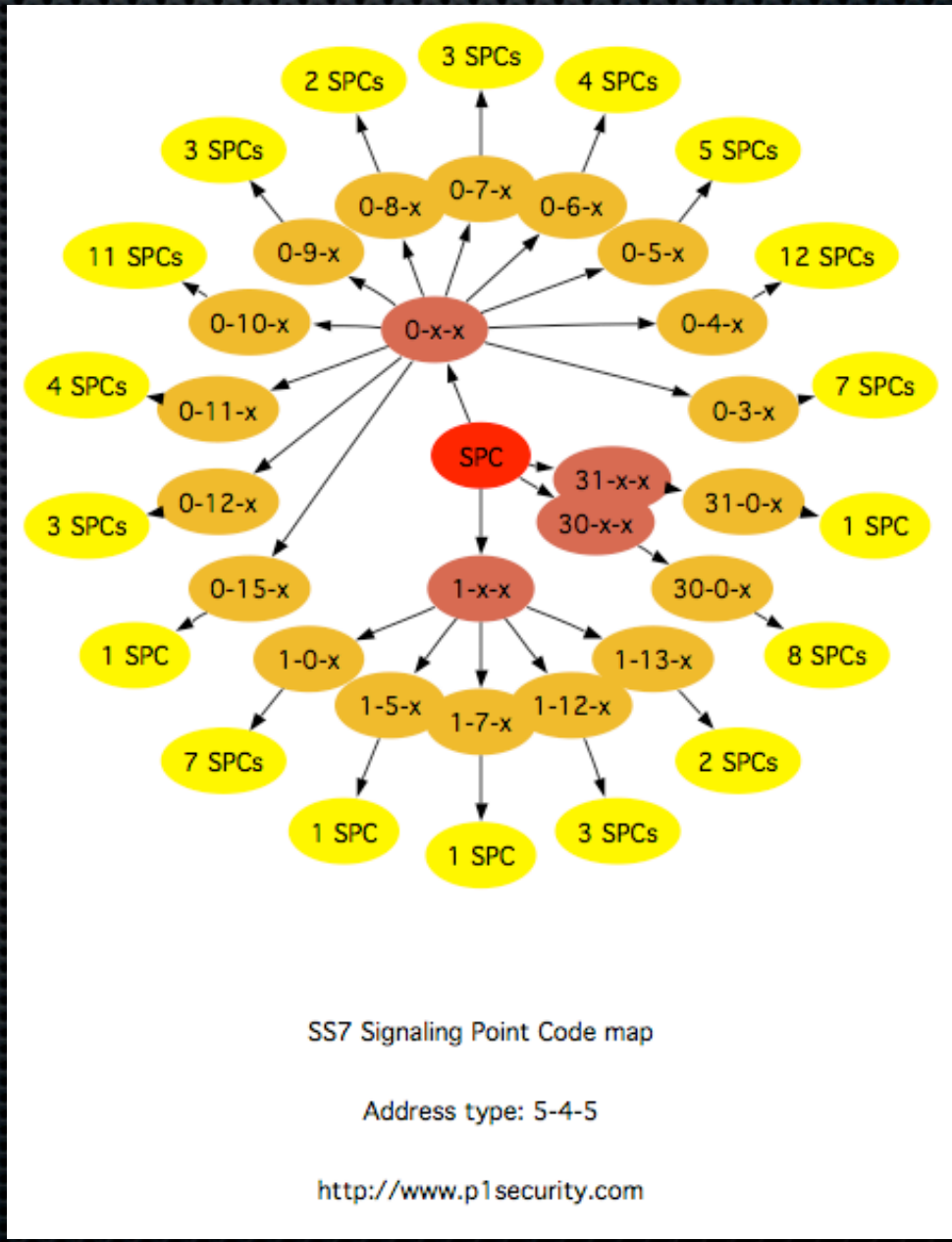


- SANC and ISPCs
- SANC assigned by ITU
- 4-2-3-5 SPCs

Confidential - (C) P1 Security 2008-2010

Scan to network maps

- Multiple formats for Point Code representation (3-8-3, NIPC, 5-4-5, Hex, Decimal)
- One Point Code “1-2-1” can represent many different addresses.
- Helps target “good” part of the network (SMSC, Testbed, HLR cluster or BSCs?)



http://www.p1security.com/

LTE scanning strategies

P1 Security
Priority One Security

- Mix between SIGTRAN scan and IP scan
- Target protocols: S1, X2
- Inter- eNodeB communications (X2)
- Communication between eNodeBs and Core Network
- Tools: SCTP connect scan, SCTPscan NG or PTA

3. Exploit

P1 Security
Priority One Security

- Standard vulnerabilities:
  - Known vulnerabilities are present, but scarce: proprietary tools, network elements, ...
  - Misconfiguration is present often: once working, people don't touch (fix) the network.
  - Simple architecture problems: HLR without SSL on OAM, logs exposed, vulnerable VLAN setup
- And unstandard / Telecom specific vulnerabilities:

ASN.1 paradise or hell

- ITU is ASN.1 addicted
- Plenty of TLV, tons of complex protocols
- Encodings:
  - Old protocols: BER, DER
  - Newer: PER, Aligned, Unaligned
- Encoding bombs, Decompression bombs
- e.g. LTE S1 protocol between eHNB and SGW, MME

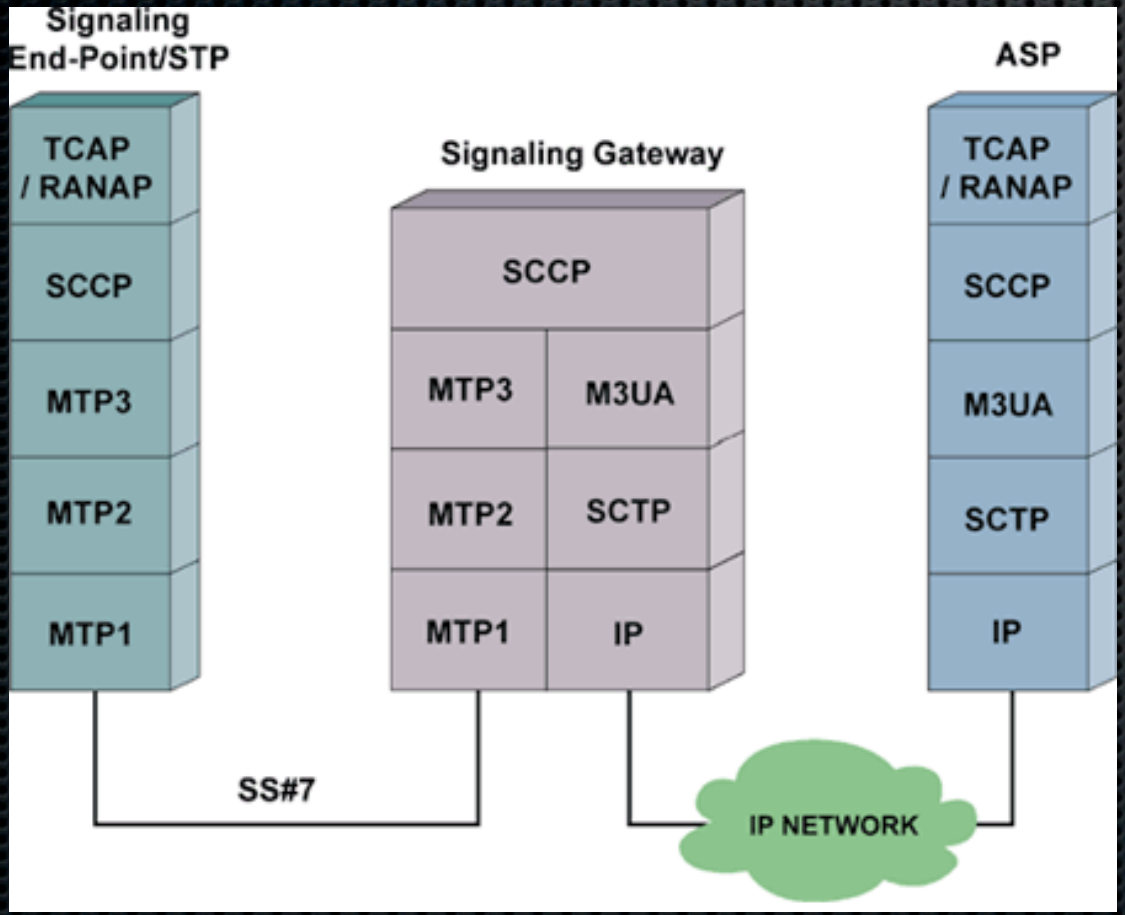
SCTP Fuzz Target

- Protocol Specification is huge
  - RFC 5062, RFC 5061, RFC 5043, RFC 4960, RFC 4895, RFC 4820, RFC 4460, RFC 3873, RFC 3758, RFC 3554, RFC 3436, RFC 3309, RFC 3286, RFC 3257, RFC 2960
- Good target for vulnerabilities
  - CVE-2010-1173 CVSS Severity: 7.1 (HIGH), CVE-2010-0008 CVSS Severity: 7.8 (HIGH), CVSS Severity: 7.8 (HIGH), CVE-2009-0065 CVSS Severity: 10.0 (HIGH), CVE-2008-4618 CVSS Severity: 7.8 (HIGH), CVE-2008-3831, CVE-2008-4576, CVE-2008-4445, CVE-2008-4113, CVE-2008-3792, CVE-2008-3526, CVE-2008-2826, CVE-2008-2089, CVE-2008-2090, CVE-2008-1070, CVE-2007-6631, CVE-2007-5726, CVE-2007-2876, CVE-2006-4535 ... CVE-2004-2013 (33 vulnerabilities)

Scapy and SCTP

- send(IP(dst="10.0.0.1")/SCTP(sport=2600,dport=2500)/SCTPChunkInit(type=1))
- send(IP(dst="10.37.129.140")/SCTP(sport=2600,dport=2500)/SCTPChunkInit(type=1)/SCTPChunkParamCookiePreservative()/SCTPChunkParamFwdTSN()/SCTPChunkParamIPv4Addr())
- send(IP(dst="10.37.129.140")/SCTP(sport=2600,dport=2500)/SCTPChunkInit(type=1)/SCTPChunkParamAdaptationLayer()/SCTPChunkParamCookiePreservative()/SCTPChunkParamFwdTSN()/SCTPChunkParamIPv4Addr()/SCTPChunkParamUnrocognizedParam()/SCTPChunkParamECNCapable()/SCTPChunkParamHearbeatInfo()/SCTPChunkParamHostname()/SCTPChunkParamStateCookie())
- It can get ugly... and i'm not even fuzzing here.

SIGTRAN Stack de-synchronization: more exposure & attacks

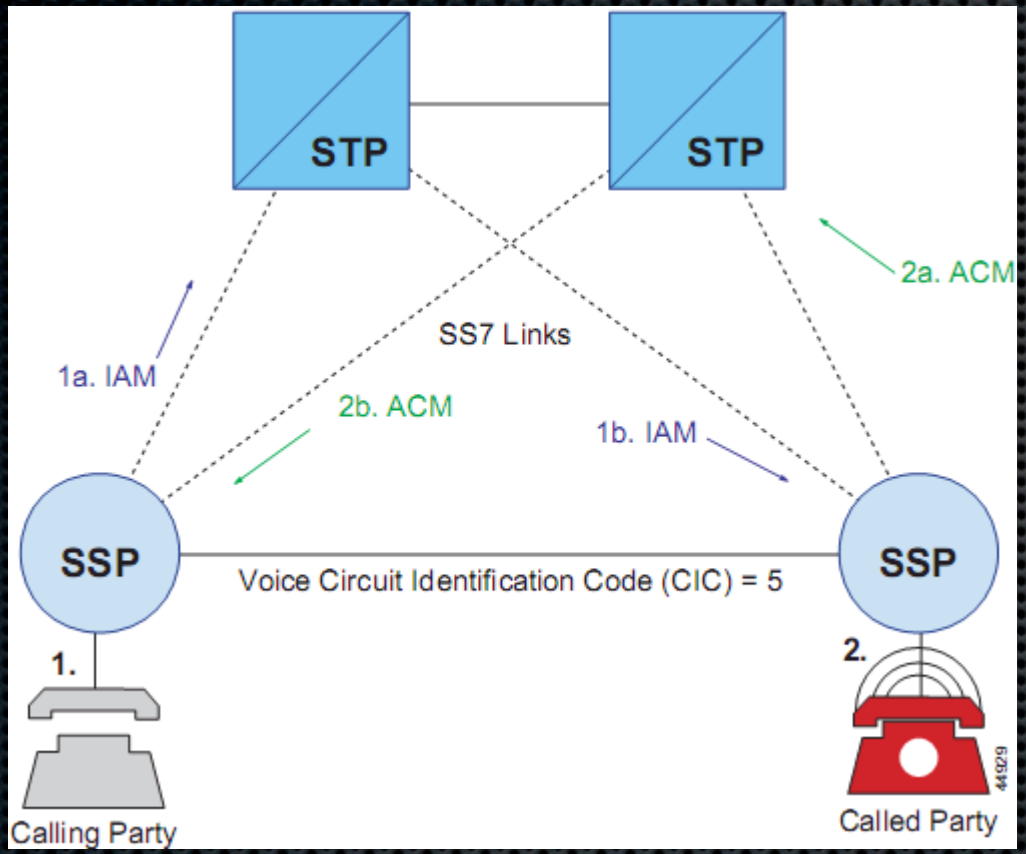


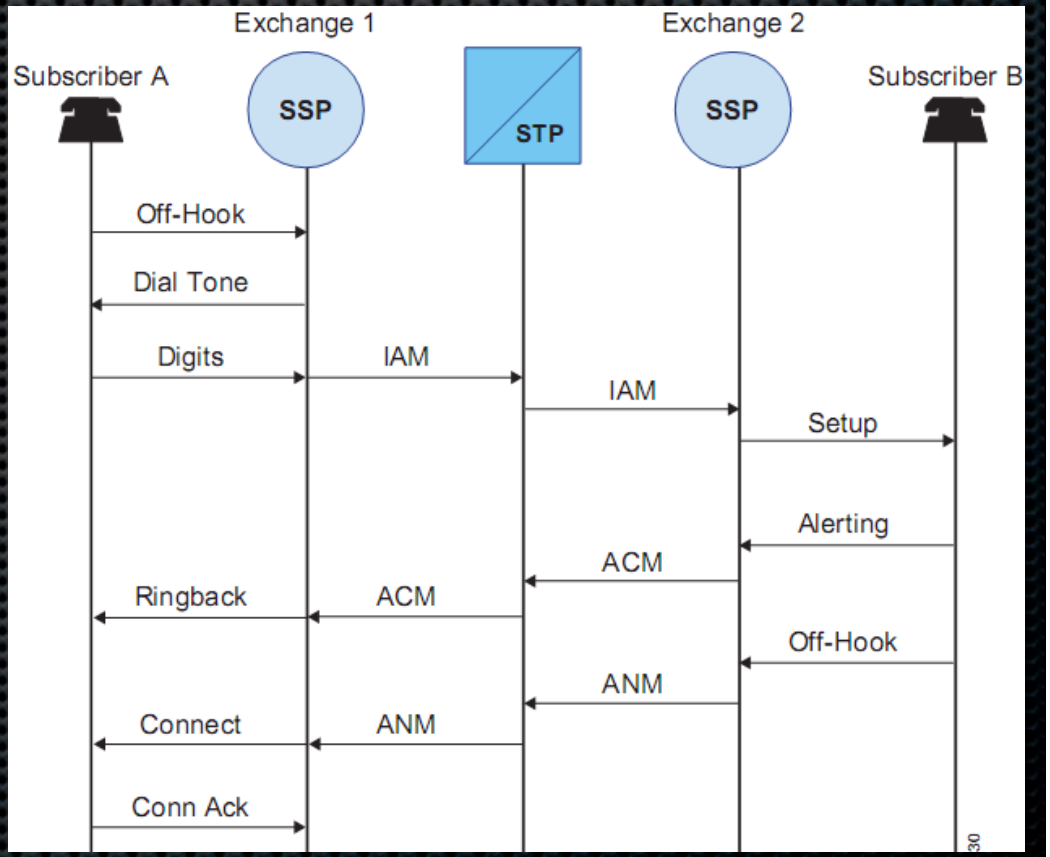
- IP/SCTP/M3UA std by IETF
- MTP3/SCCP/TCAP std by ITU
- Finite State Machine in M3UA can be tricked into believing you're a peer.
- Once you're signaling peer you can…

P1 Security
Priority One Security

SS7 ISUP Call Initiation Flow

IAM attack: Capacity DoS





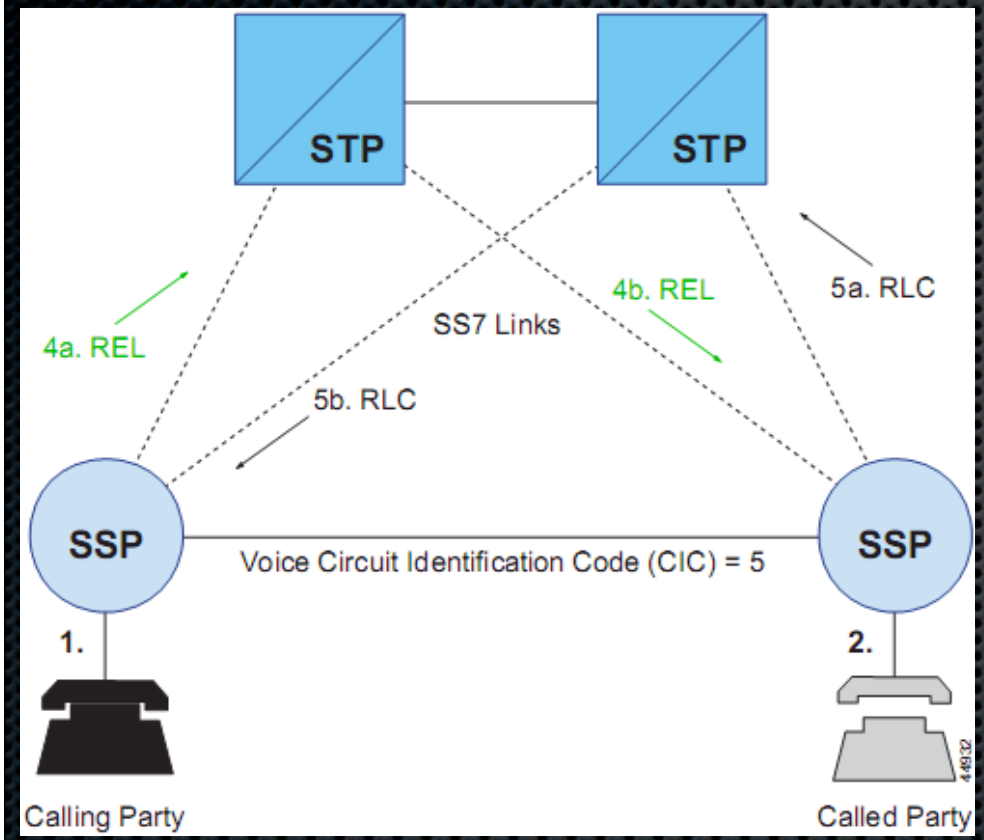
Attack Quiz!

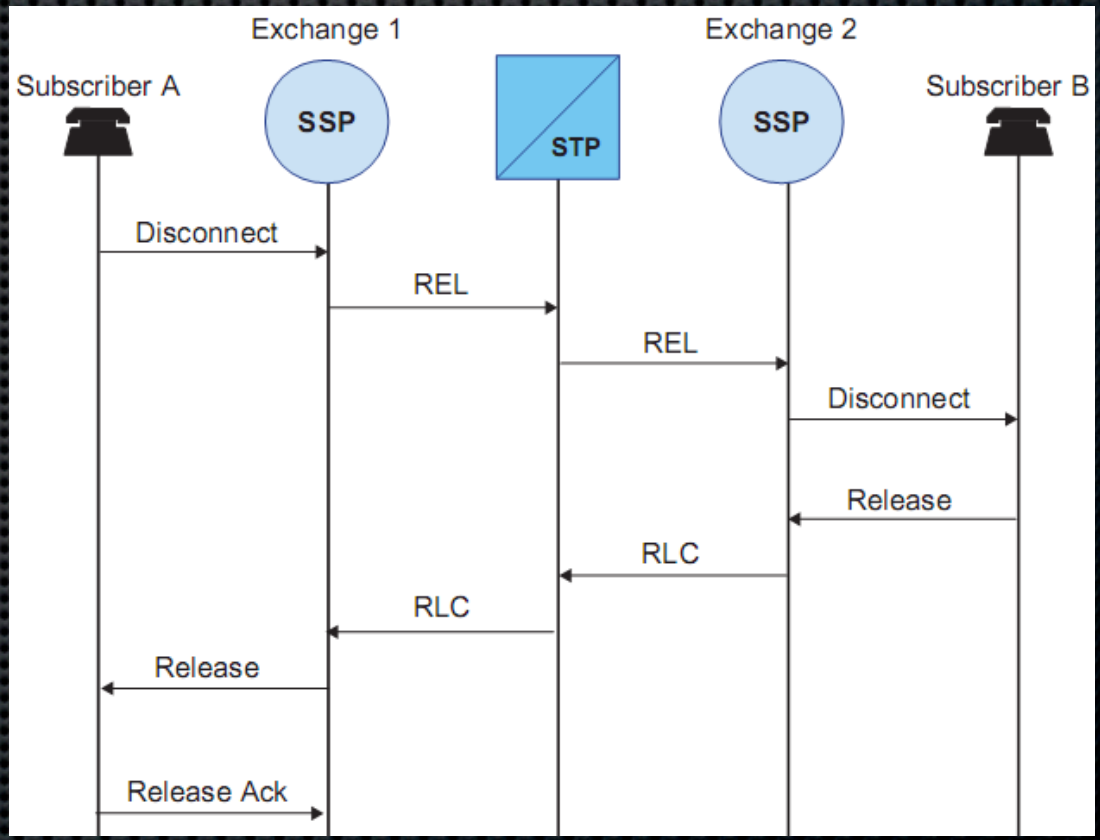
http://www.p1security.com/

SS7 ISUP Call Release Flow

P1 Security
Priority One Security

REL attack: Selective DoS

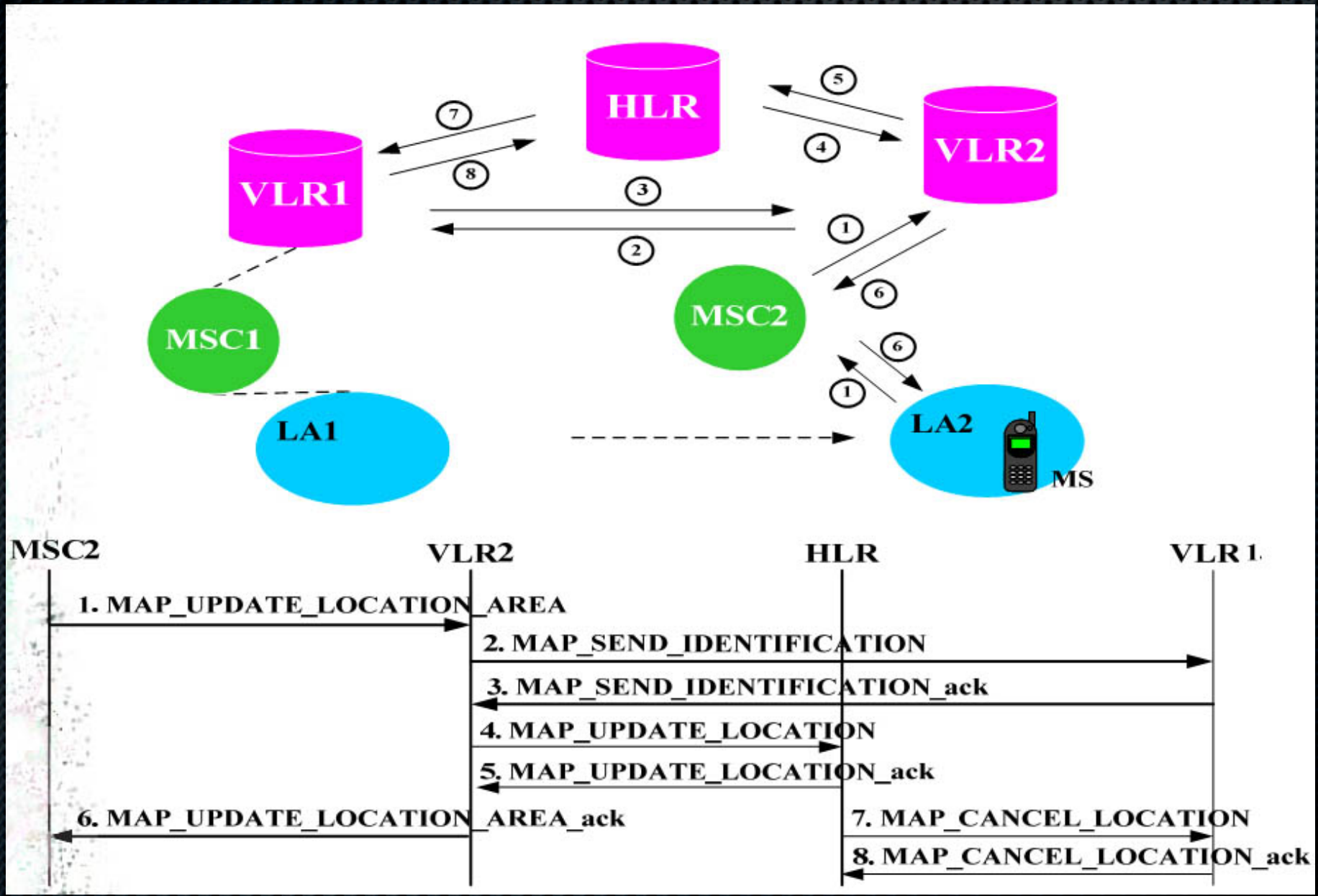




Attack Quiz!

http://www.p1security.com/

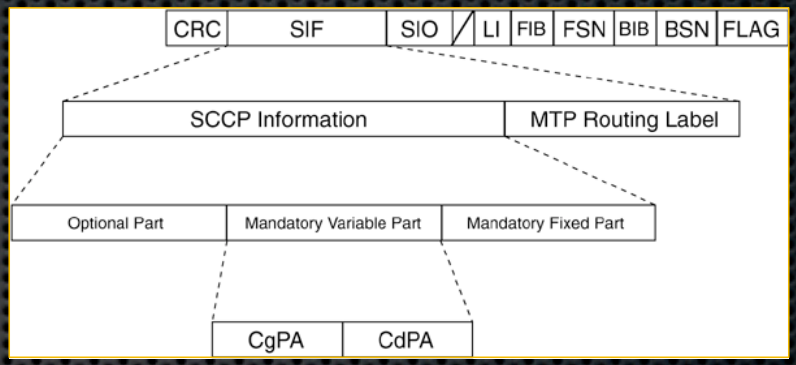
User targeted DoS



http://www.p1security.com/

Sending hostile MSU (MAP)

- Sent from any network (in the world)
- to any target mobile phone
- HLR Lookup may be used to prepare attack (IMSI gathered through SRI_for_SM)
- Phone is registered on network, can make call, cannot receive calls or SMS.



IMSI scanning / querying needed !

```
GSM Mobile Application
  Component: invoke (1)
    invoke
      invokeID: 1
      opCode: localvalue (0)
        localvalue: updateLocation (2)
      imsi: 520092999999999F9
      TBCD digits: 250029999999999
      msc-Number: 91839099999999
        1... .... = Extension: No Extension
        .001 .... = Nature of number: International Number (0x01)
        .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
        Address digits: 380999999999
        Country Code: 380 Ukraine length 3
      vlr-Number: 91839099999999
        1... .... = Extension: No Extension
        .001 .... = Nature of number: International Number (0x01)
        .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
        Address digits: 380999999999
        Country Code: 380 Ukraine length 3
      vlr-Capability
        Padding: 4
        supportedCamelPhases: C0 (phase1, phase2)
        Padding: 4
        supportedLCS-CapabilitySets: F0 (lcsCapabilitySet1, lcsCapabilitySet2, lcsC
```

http://www.p1security.com/

Attack success

P1 Security
Priority One Security

```
GSM Mobile Application
  Component: invoke (1)
    invoke
      invokeID: 1
      opCode: localValue (0)
        localValue: insertSubscriberData (7)
      msisdn: 919799999999F9
        1... .... = Extension: No Extension
        .001 .... = Nature of number: International Number (0x01)
        .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
        Address digits: 79999999999
        Country Code: 7 Russian Federation,Kazakstan length 1
      category: 0A
      subscriberStatus: serviceGranted (0)
      teleserviceList: 4 items
        TeleserviceList: shortMessageMO-PP (34)
        TeleserviceList: shortMessageMT-PP (33)
        TeleserviceList: emergencyCalls (18)
        TeleserviceList: telephony (17)
      provisionedSS: 3 items
        Ext-SS-InfoList: forwardingInfo (0)
        Ext-SS-InfoList: forwardingInfo (0)
        Ext-SS-InfoList: forwardingInfo (0)
```

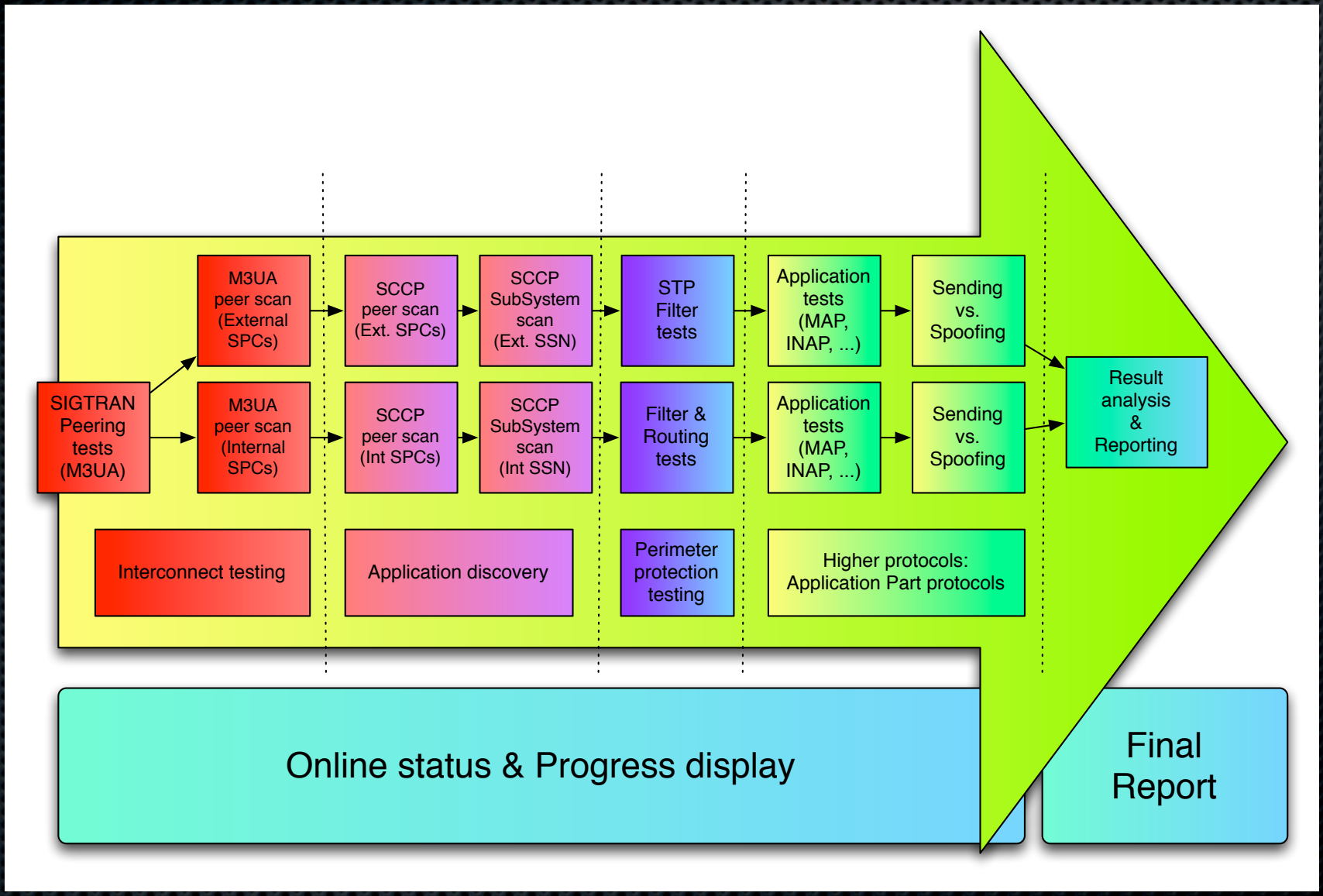
P1 Security
Priority One Security

Fuzzing, research and DoS

- Fuzzing only in testbed environment
- Because it's easy to DoS equipments
- Telecom developer obviously don't think like hackers
  - MGW: hardcoded Backdoor found in OAM terminal
  - eNodeB: protocol flaw leads to DoS
  - HLR/HSS: DB/Directory protocol leads to DoS + Diameter flaw
- Equipments are rarely tested before integration/production

P1 Security
Priority One Security

Complete audit process



http://www.p1security.com/

4. Detect & Protect

P1 Security
Priority One Security

- IP IDS don't detect these problems
- Previous Lack of IDS for telecom networks
- Fraud Management Systems target only CDR: bills, statistical analysis
- DShield.org don’t log SCTP attempts
- “netstat -anp” doesn’t list SCTP associations
- hard to track! We’re building tools to help.

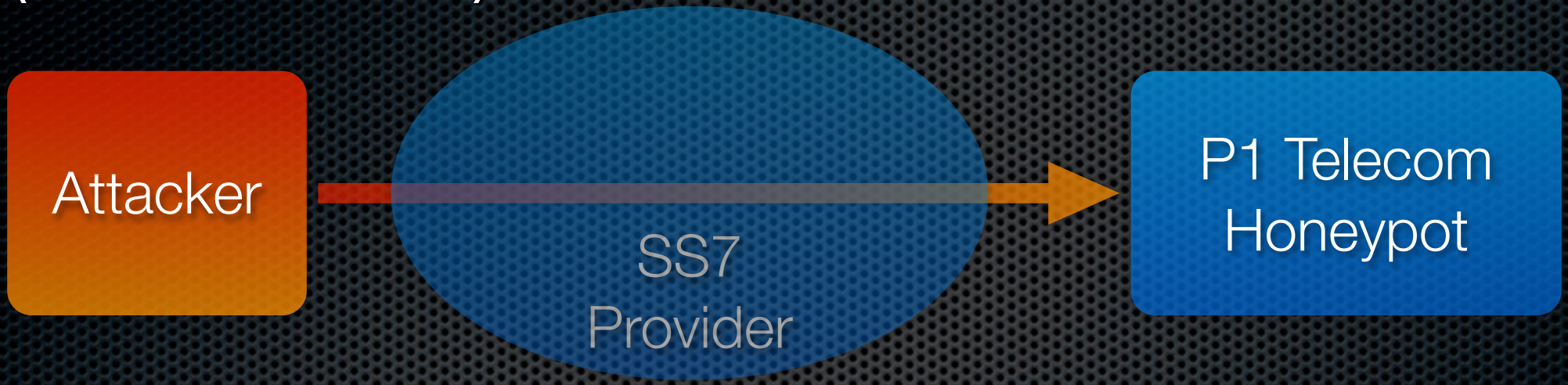
Tales of Telecom Honeypots

P1 Security
Priority One Security

- Fraud and attacks in telecom is mostly stealth
  - But the impact is massive (100k to 3 million Euro per incident is typical)
- Telecom engineers mindset is not as open for proactive security as in IP crowds
  - Prefer not to do anything and suffer from attacks
  - “If nothing is there to detect attacks, there are no attacks”
- Lack of threat intelligence in the telecom domain

SS7 Honeypot Deployment (standalone)

P1 Security
Priority One Security



Attacker who tries to conduct fraud on the target system

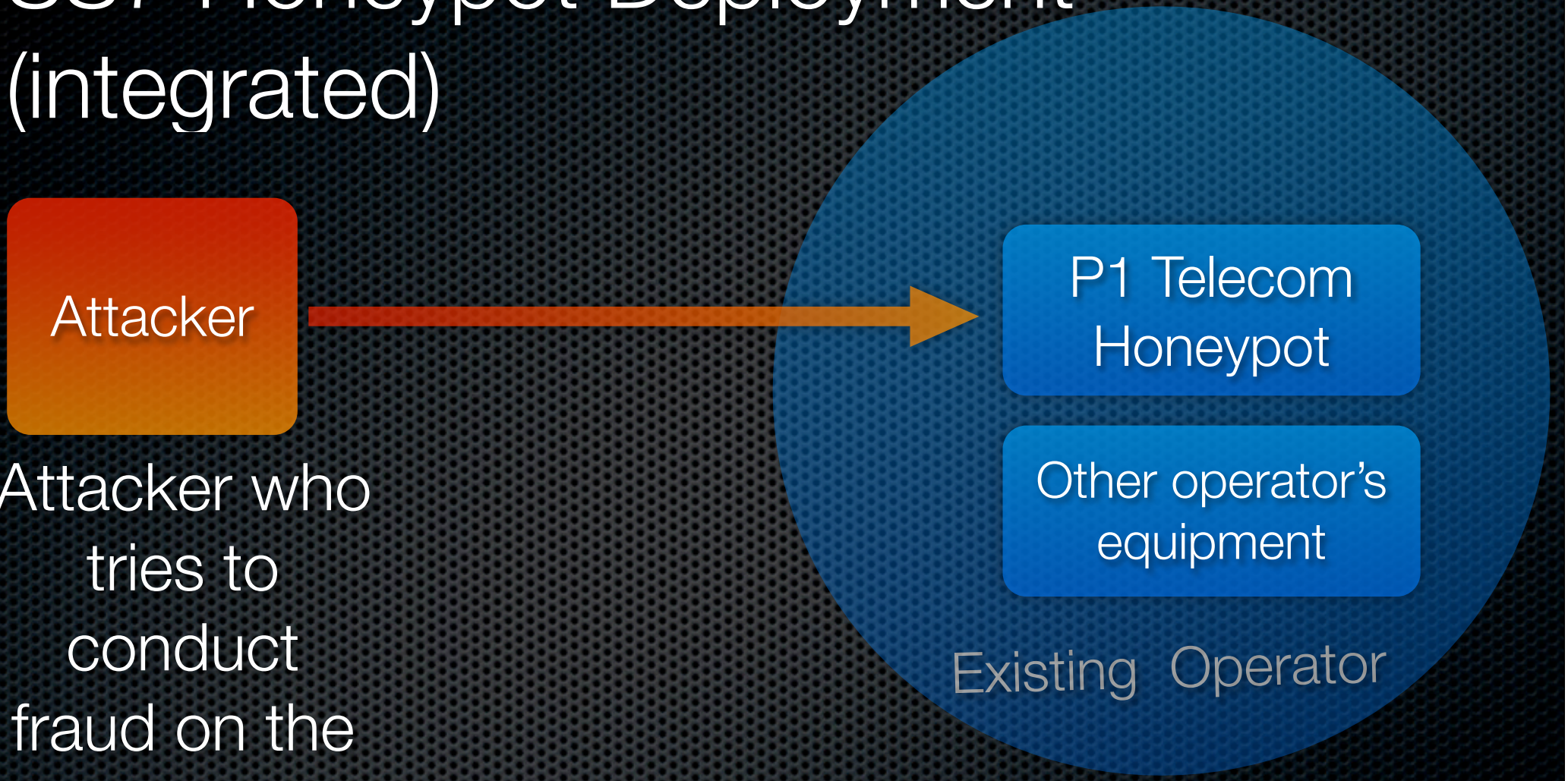
SS7 Provider who manages SS7 links (like ISP)

SS7 Honeypot with SS7 link and address (pointcode or SPC)

Confidential - (C) P1 Security 2008-2010

SS7 Honeypot Deployment (integrated)

P1 Security
Priority One Security

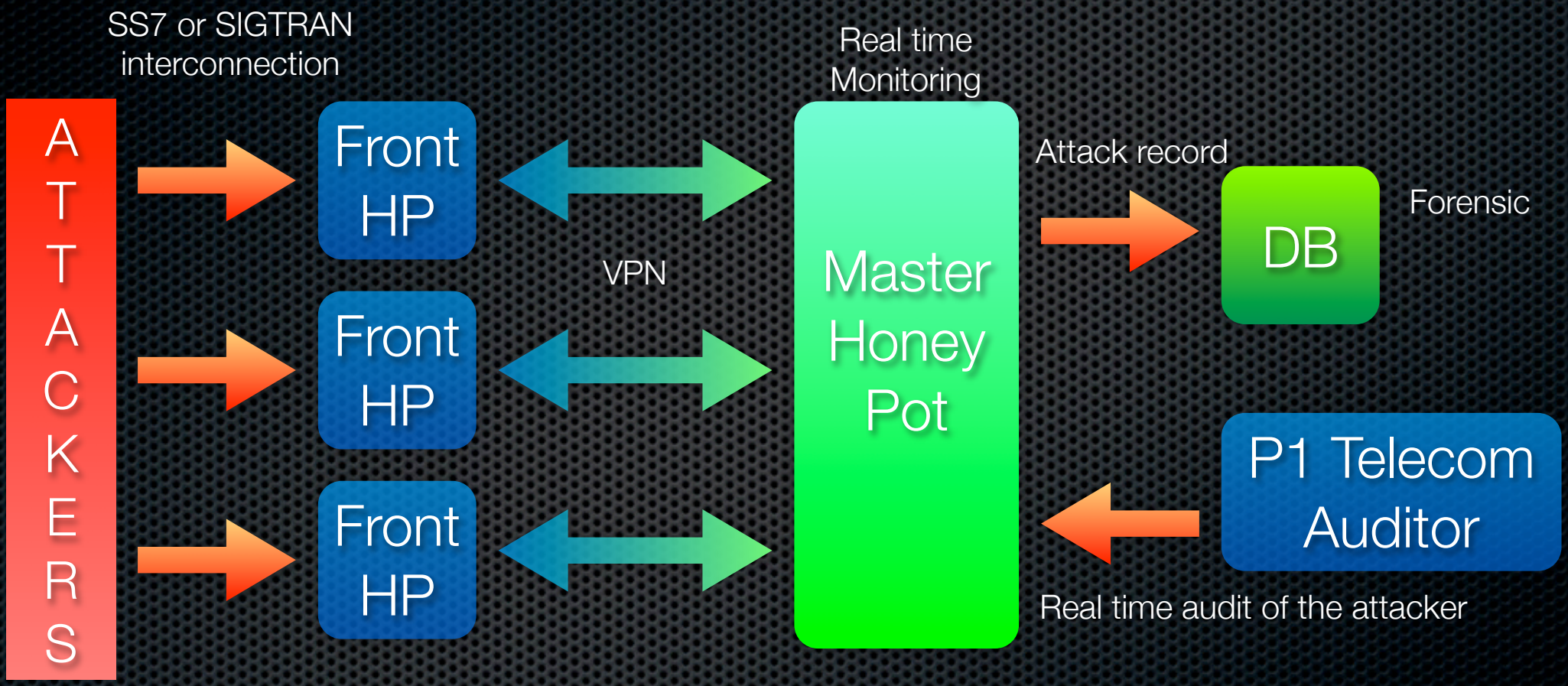


Attacker who tries to conduct fraud on the operator's system

SS7 Honeypot within operator SS7 network

Confidential - (C) P1 Security 2008-2010

Architecture



- Interconnection is like a VPN, always two-way
- If attackers does requests (interco), we can request too
- We conduct scan with P1 Telecom Auditor through interco.

Confidential - (C) P1 Security 2008-2010

Detection results

- Realtime detection of scans (IDS)
  - SIGTRAN scans
  - SS7 scans
- Detection of telecom specifics
  - SIM Boxes (subscription fraud),
  - traffic steering and anti-steering packets/techniques
  - Illegal traffic routing (mostly SMS, never seen before by operator, “lost in traffic”)

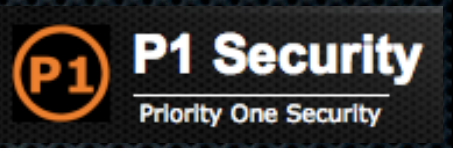
Honeypot results

- Threat intelligence!
- Nice attacker fingerprints:
  - Single node attackers (stack on one system)
  - Whole carrier infrastructure attacking (insider? relay? approved?)
- Helps the blacklisting of IDs, Phone numbers, …
- And identification of the fraudsters

Conclusions

- End of walled garden era, more exposed:
- High Exposure in term of IP-reachability (starting in 3G/IMS) and reachability of the IP-equipment (specifically in LTE networks)
- Network complexity (planes/layers) and protocol diversity make it very hard to get right from the beginning.
- Few “dare” to audit / test their telecom environment.
- Tools and services are now mature and efficient.
- First need to visualize the problem: discovery, awareness.

Credits



- Everybody from Telecom Security Task Force
- Fyodor Yarochkin
- Emmanuel Gadaix
- Raoul Chiesa
- Daniel Mende, Rene Graf, Enno Rey
- Everyone at P1 Security and P1 Labs

http://www.p1security.com/

Thank you!

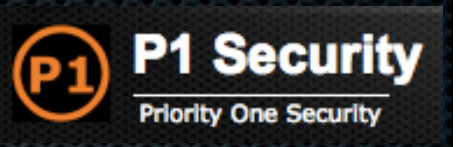
P1 Security
Priority One Security

Questions?

Ask:

Philippe.Langlois@p1sec.com

http://www.p1security.com/

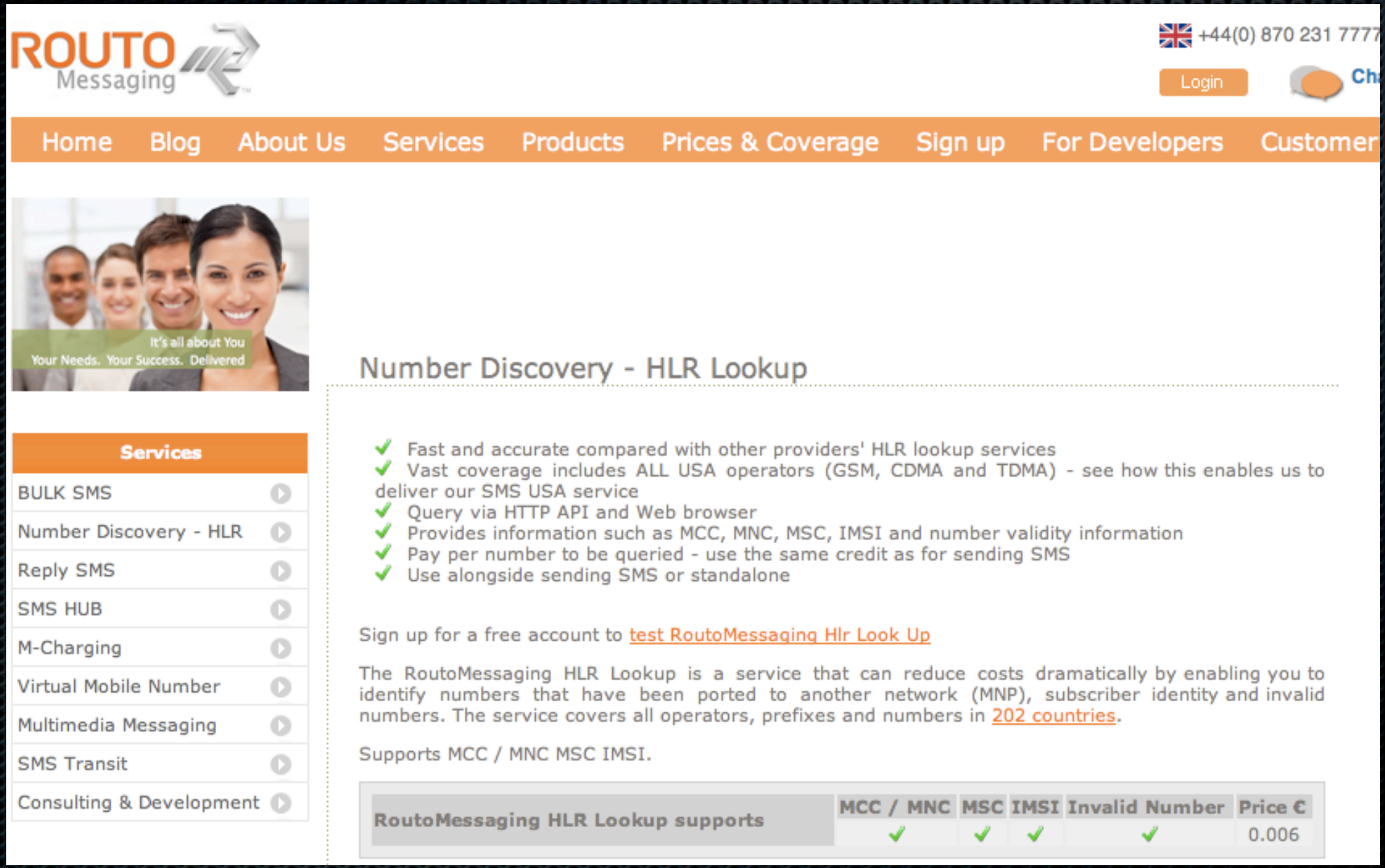


http://www.p1security.com/

Backup slides

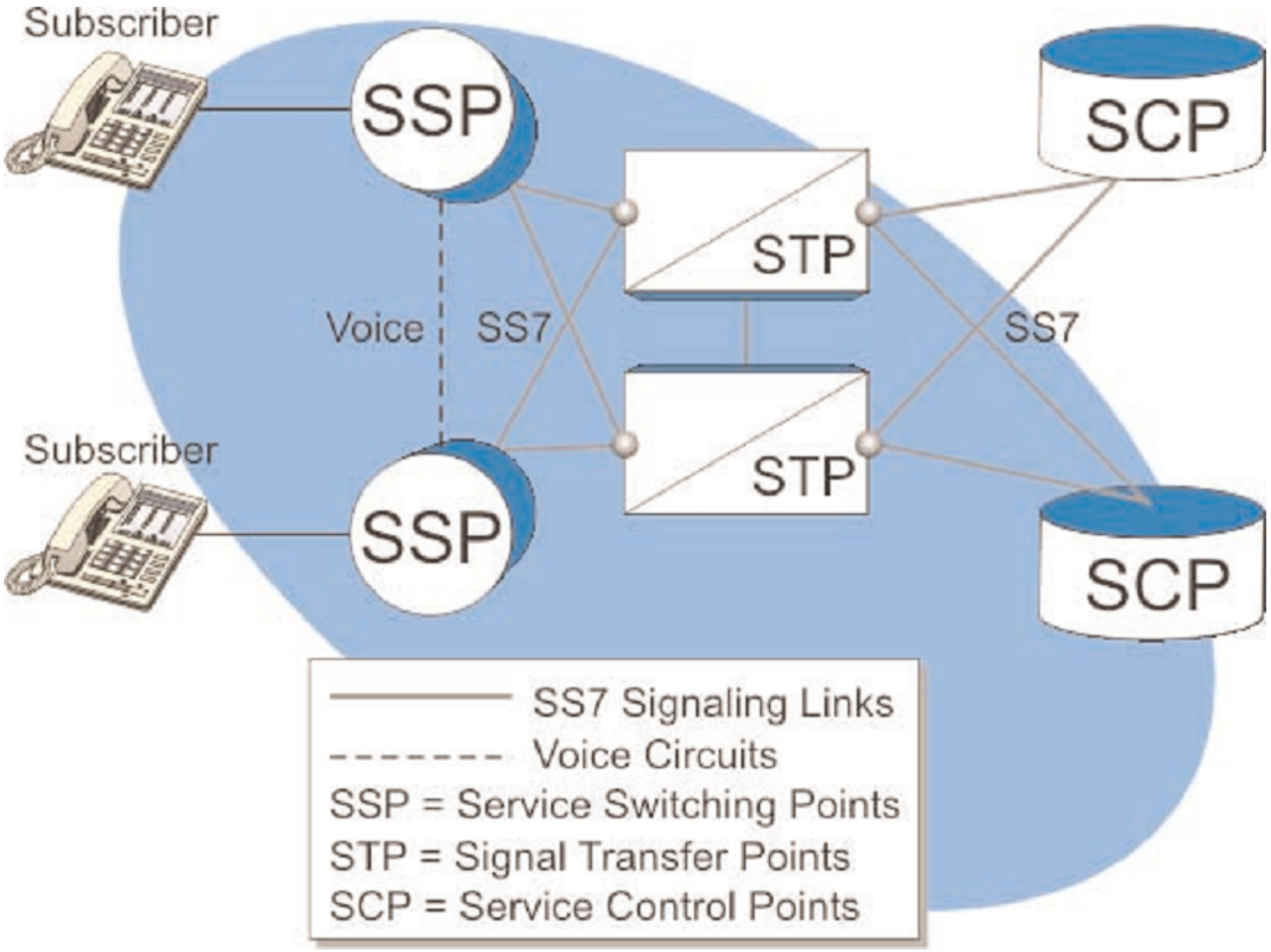
P1 Security
http://www.p1sec.com

HLR Lookups



Confidential - (C) P1 Security 2008-2010

SS7 basic architecture

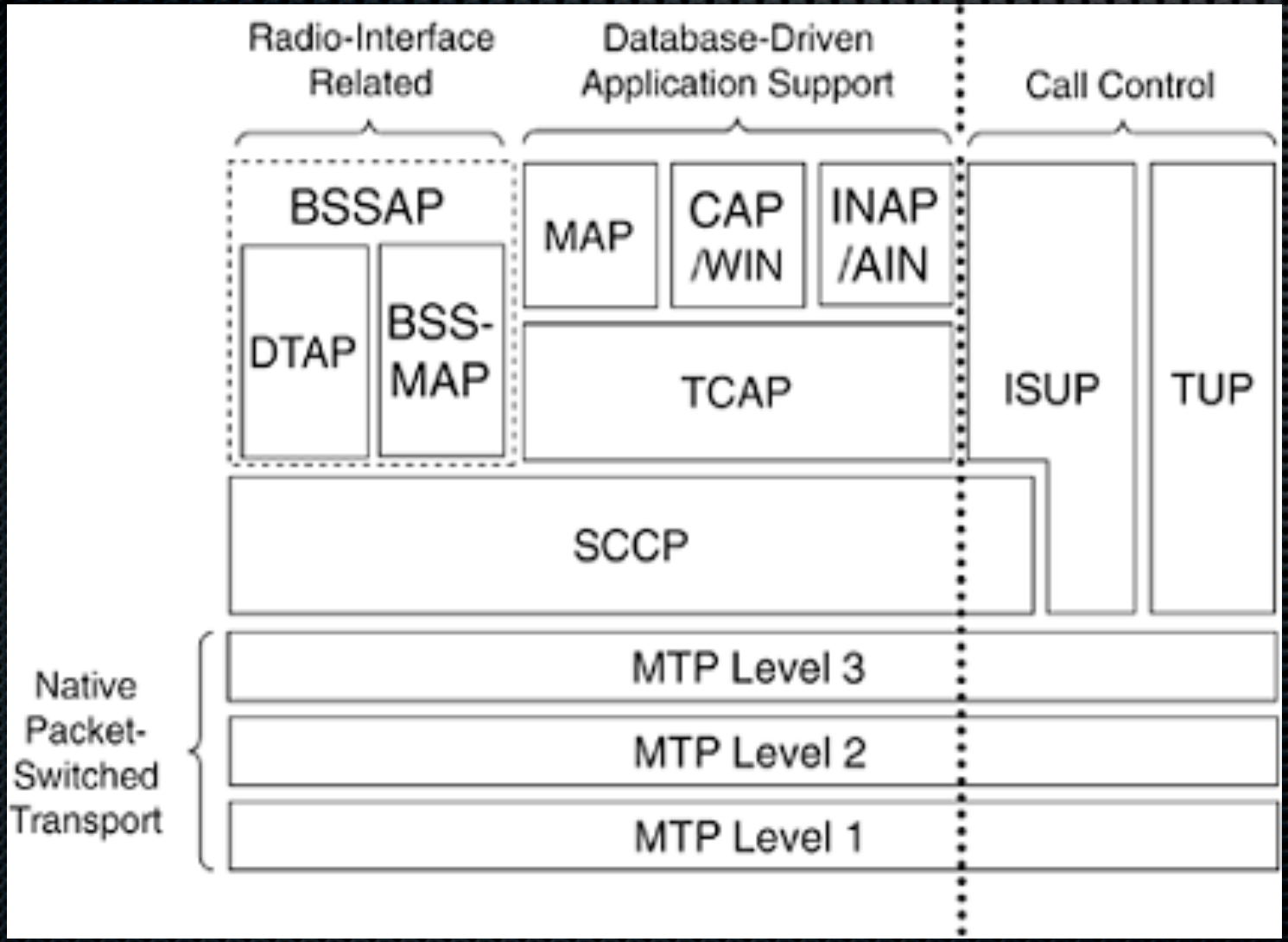


P1 Security
Priority One Security

Basic SS7 network elements

- **Service Switching Points** (SSP) are the telephone "switches" that are interconnected to each other by SS7 links. The SSPs perform call processing on calls that originate, tandem, or terminate at that site.
- **Signal Transfer Points** (STP) are "routers" that relay messages between network switches and databases. Their main function is to route SS7 messages to the correct outgoing signaling link, based on information contained in the SS7 message address fields.
- **Service Control Points** (SCP) contains centralized network databases for providing enhanced services. Examples of services include toll-free numbers and prepaid subscriptions.

Under the hood: SS7 stack



Confidential - (C) P1 Security 2008-2010

P1 Security
Priority One Security

Problem

- Mobile Network Operators and other Telecom Operators
  - use Fraud Management System that are reactive only, only see fraud when it has stolen money from the operator,
  - have no way to tell if their network weaknesses are,
  - must wait for fraud, network downtime, crashes, spam, intrusions to happen in order to see how it happened.
- Governments, safety agencies and telecom regulators
  - have no way to assess the security, resiliency and vulnerability of their Telecom Critical Infrastructure

P1 Security Solution

- PTA gives vision on Telecom signaling networks (SS7, SIGTRAN, LTE sig), a security perimeter previously without technical audit.
- Telecom and Mobile Operator can scan and monitor their signaling perimeter as they do for their Internet and IP perimeter, detecting vulnerabilities before hackers, fraudsters and intruders do.
- Delivers metric for management, reports and fixes for experts.
- Right now, all the following problems go undetected (next pages) and could be detected with PTA:

P1 Solution Portfolio

P1 Security
Priority One Security

	Awareness	Security Planning	Monitoring & Detection	Intelligence & Response	Quality Audit
PRODUCTS	P1 Network Discovery	P1 Security Recorder	P1 Telecom Monitor	P1 Telecom Honeypot	P1 Telecom Auditor
SERVICES	Telecom Security Audit	Basic security Assistance	MSP Assistance	Forensic Assistance	Auditor Assistance
	Telecom Security Training			TCERT	

http://www.p1security.com/

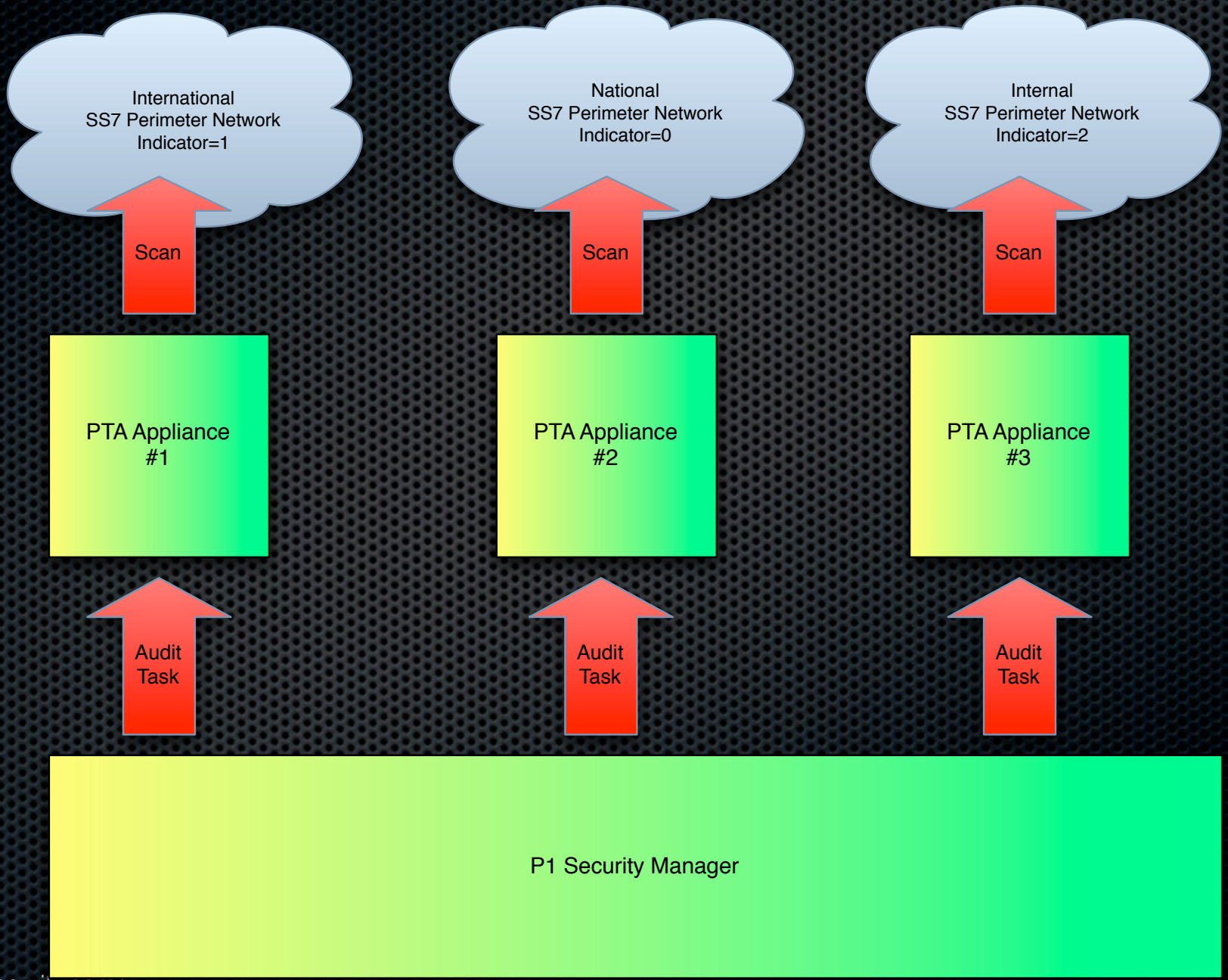
How?

P1 Security
Priority One Security

- P1 Security Telecom Auditor service delivered over the web as SaaS (Software as a Service) or Appliance + Private Cloud
- Appliances delivered to MSP or Customer (Virtual Machine with PTA Probe software)
- Available internal experts to help interpret the results if requested. External professional network to help remediate the problems.

http://www.p1security.com/

PTA Deployment



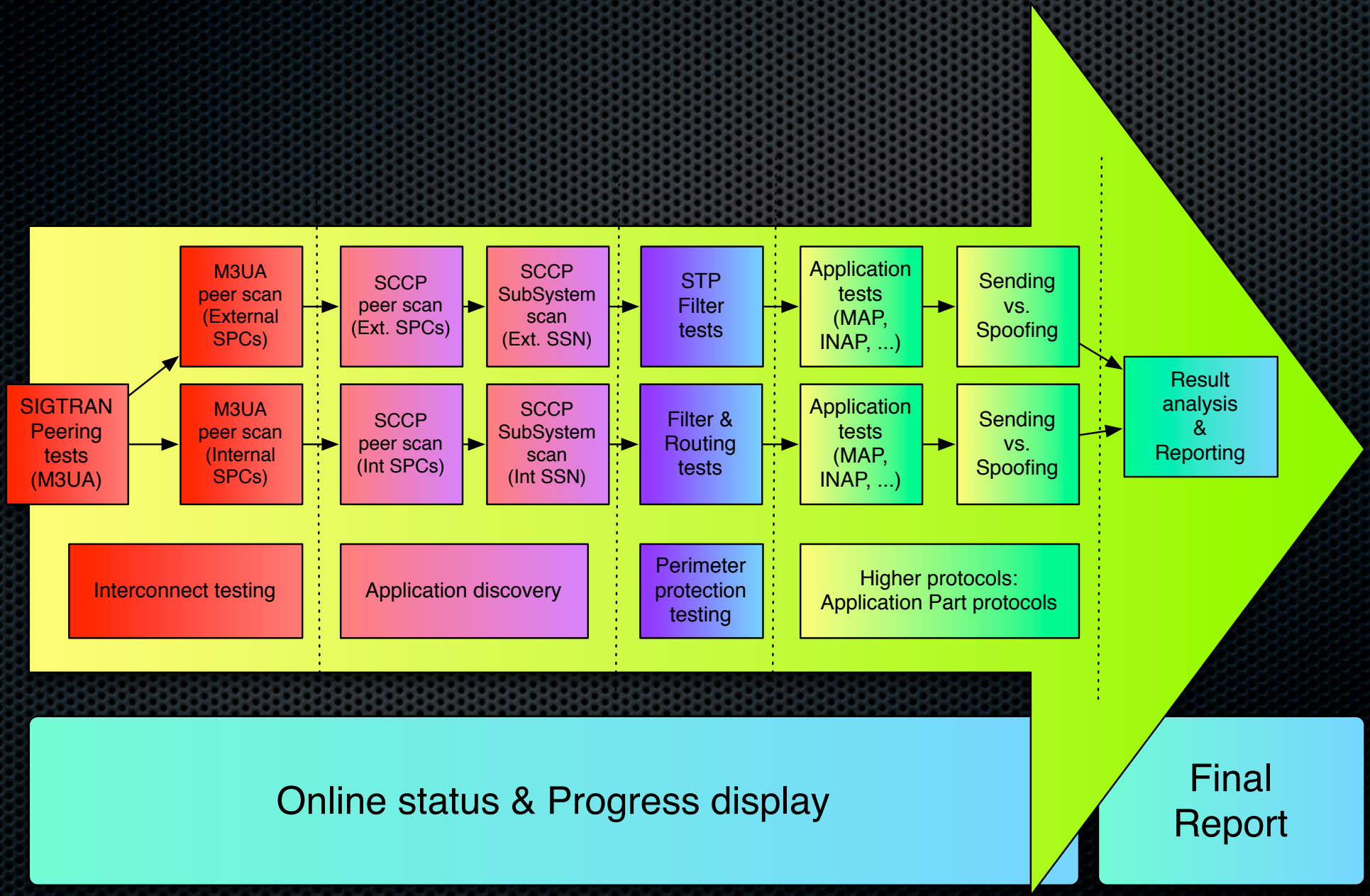
P1 Security
Priority One Security

PTA Audits

- PTA Audits simulate human analysis of a SS7 signaling network.
  - It is composed of a set of signaling tests each representing one category of attack scenario or one specific attack or fraud attempt.
  - The Test Knowledge Base is constantly updated with new attack scenarios.
- The behavior, strategy and analysis of the Audit results is driven by a Machine Learning engine using SVM methods to mimic the intelligence of a human expert.

P1 Security
Priority One Security

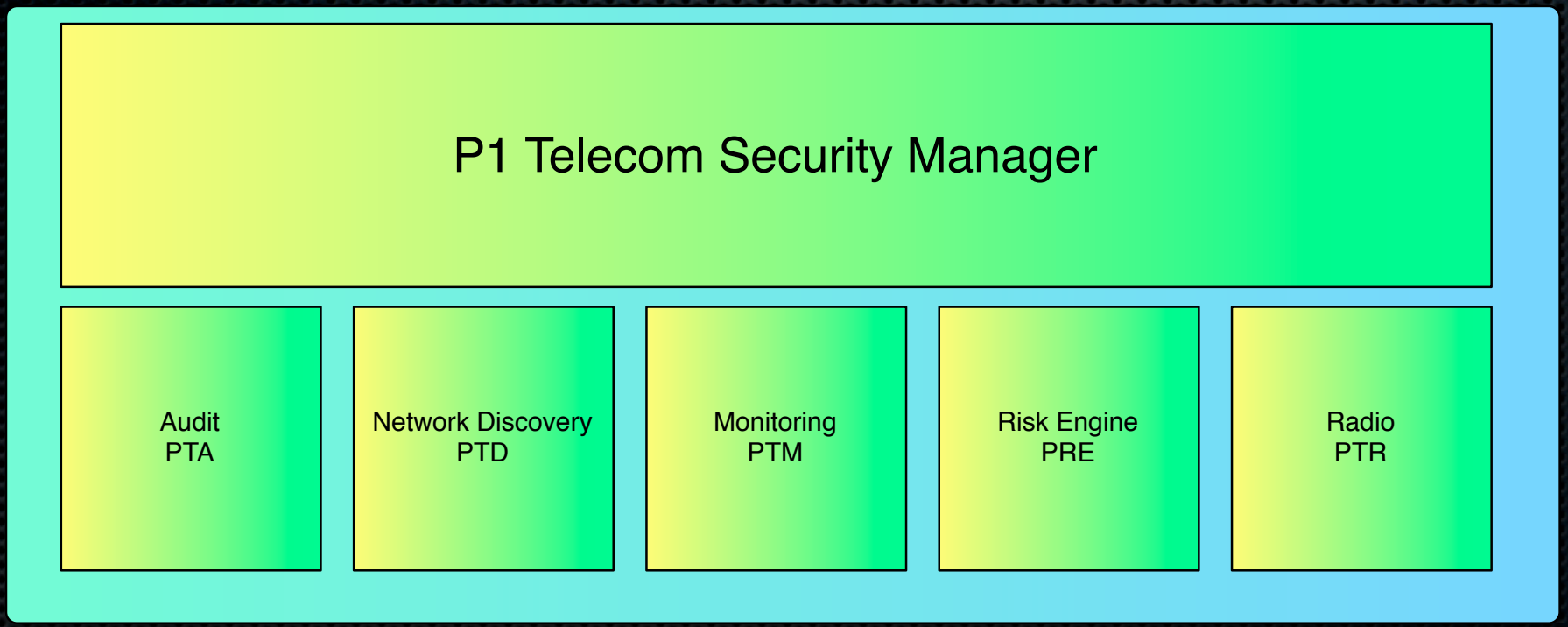
PTA Audit process



http://www.p1security.com/

P1 Products Architecture

P1 Security
Priority One Security

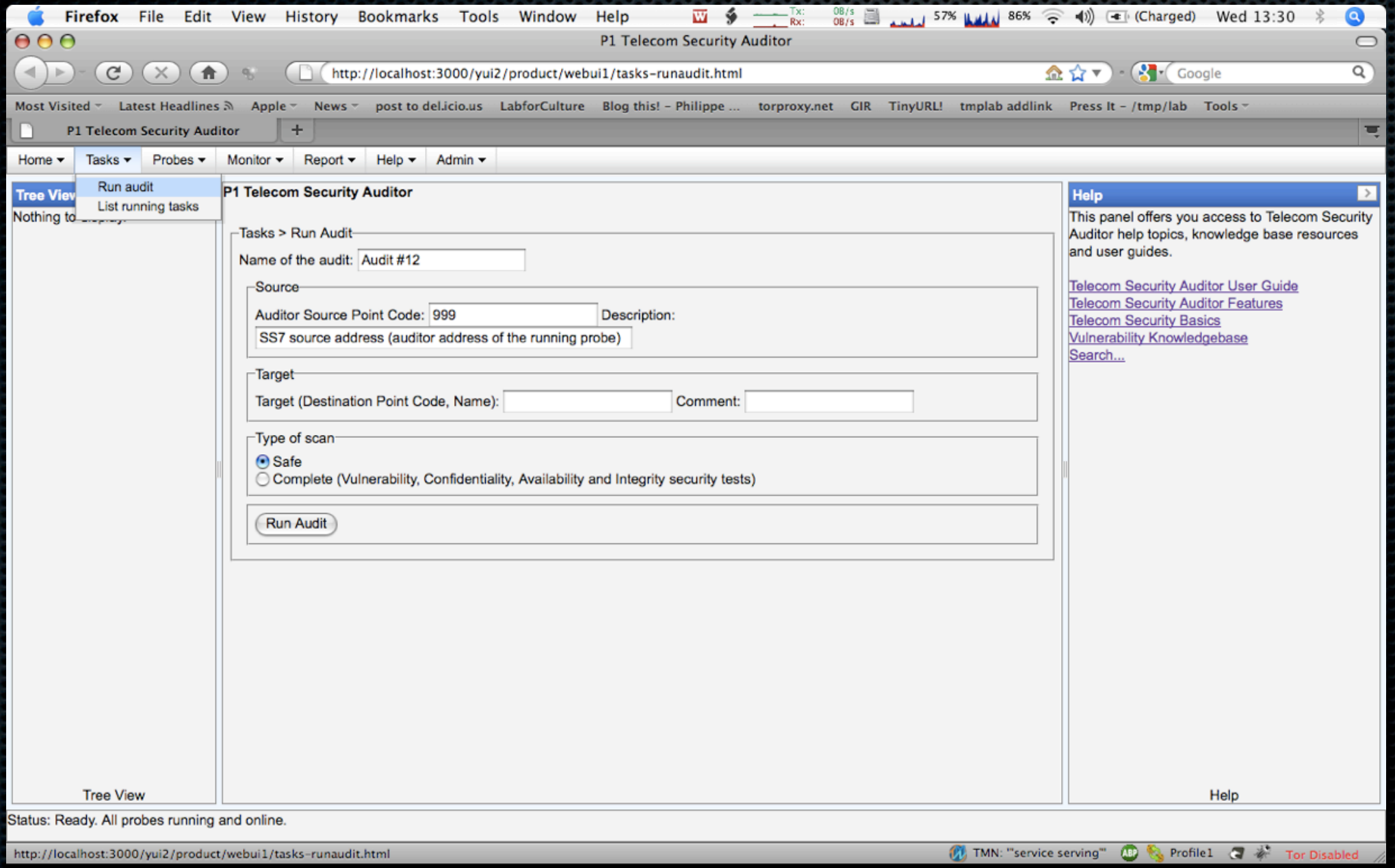


Use case	SS7 Security Audit	SS7 Active discovery	SS7 Security Monitoring	telecom risk rating	Radio perimeter security audit
Target	Telecom & Mobile operator	Telecom service provider	Telecom & Mobile operator	SS7 mbank/ mcommerce	Mobile operators

http://www.p1security.com/

P1 Security
Priority One Security

Web Access: Easy & Standardized



http://www.p1security.com/

Management

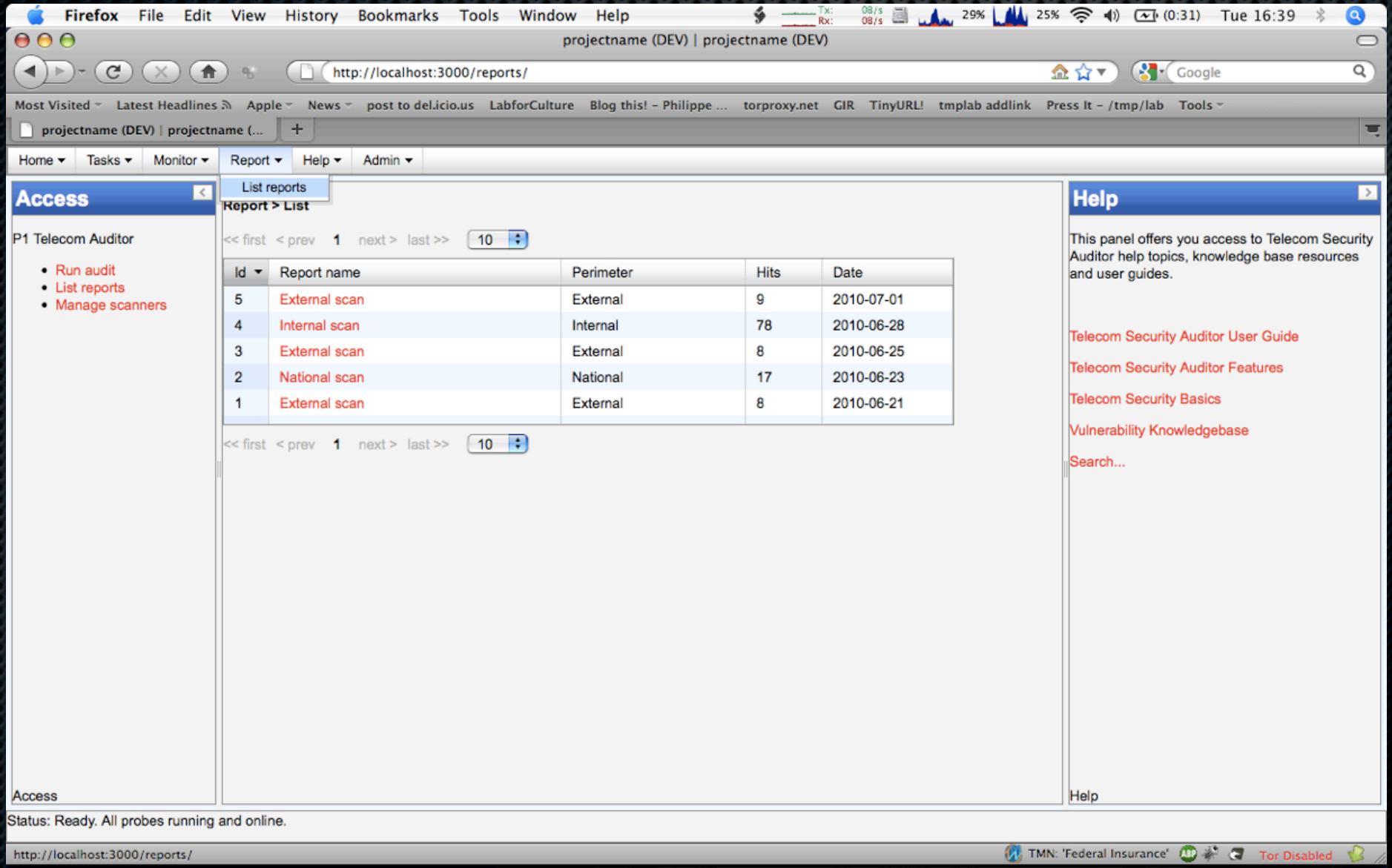
P1 Security
Priority One Security

- Dashboard
- Graphical trends and reports
- Access control from the web
- Alerts
- Multilevel Security (database encryption, SSL)

http://www.p1security.com/

Report Management

P1 Security
Priority One Security



http://www.p1security.com/

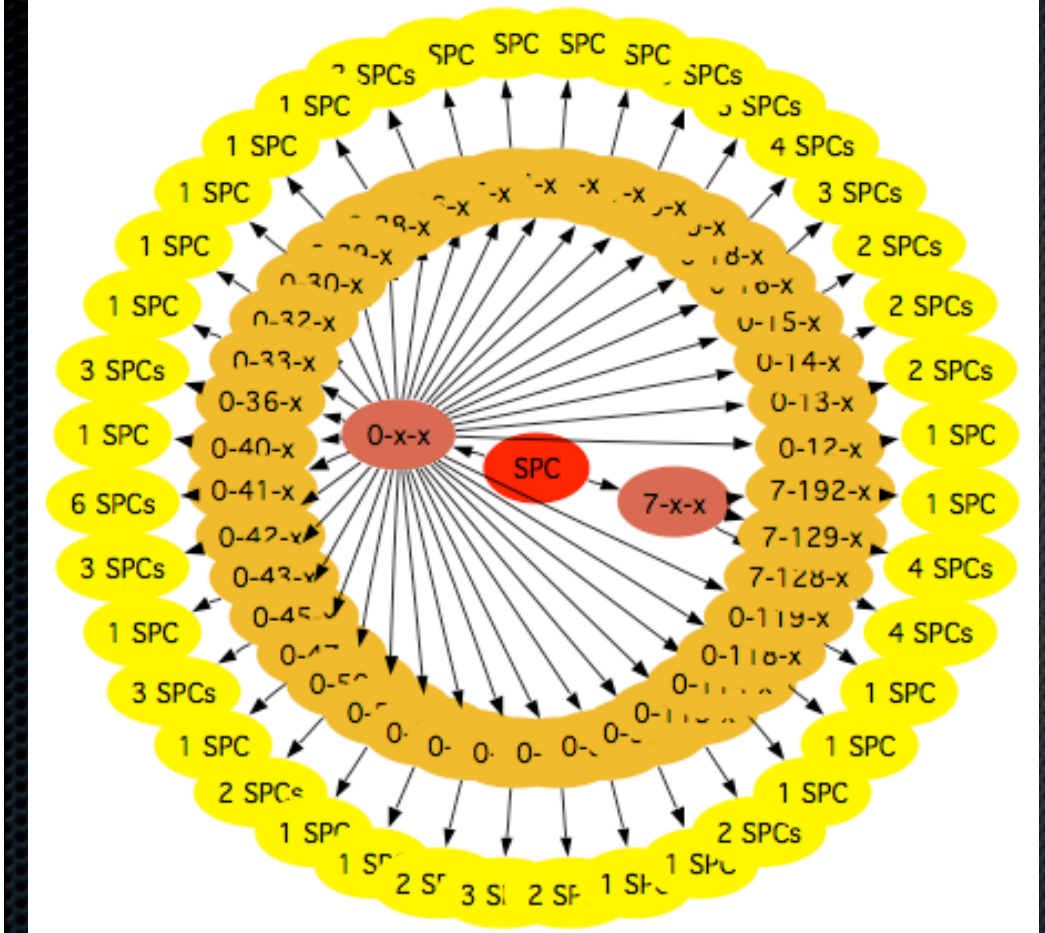
Technical

P1 Security
Priority One Security

- Needs an appliance or virtual appliance in the signaling domain
  - Requires a Signaling Point Code per perimeter
  - Multiple level of audits depending on the tested perimeter (testbed only, external, national, peer, internal network, BSS)
- Non-intrusive (safe mode)
- Zero impact on infrastructure

P1 Security
Priority One Security

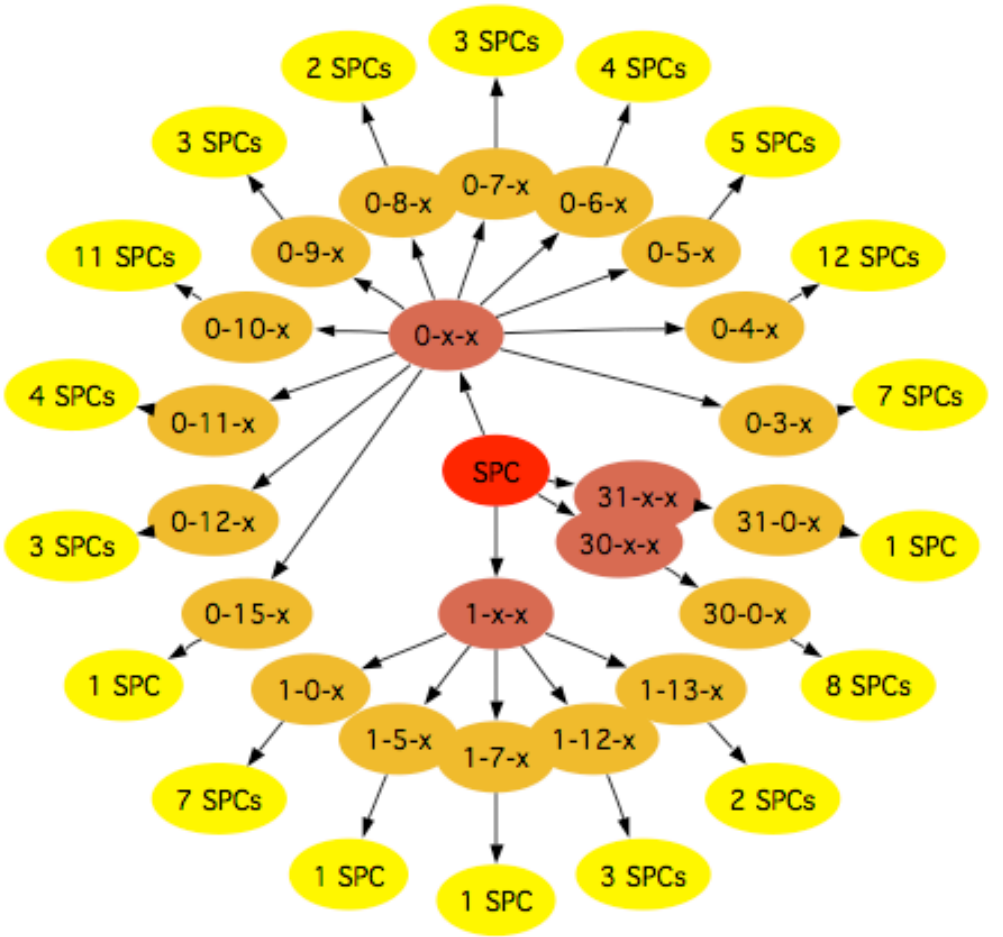
Network Map in Reports



SS7 Signaling Point Code map

Address type: 3-8-3

http://www.p1security.com



SS7 Signaling Point Code map

Address type: 5-4-5

http://www.p1security.com

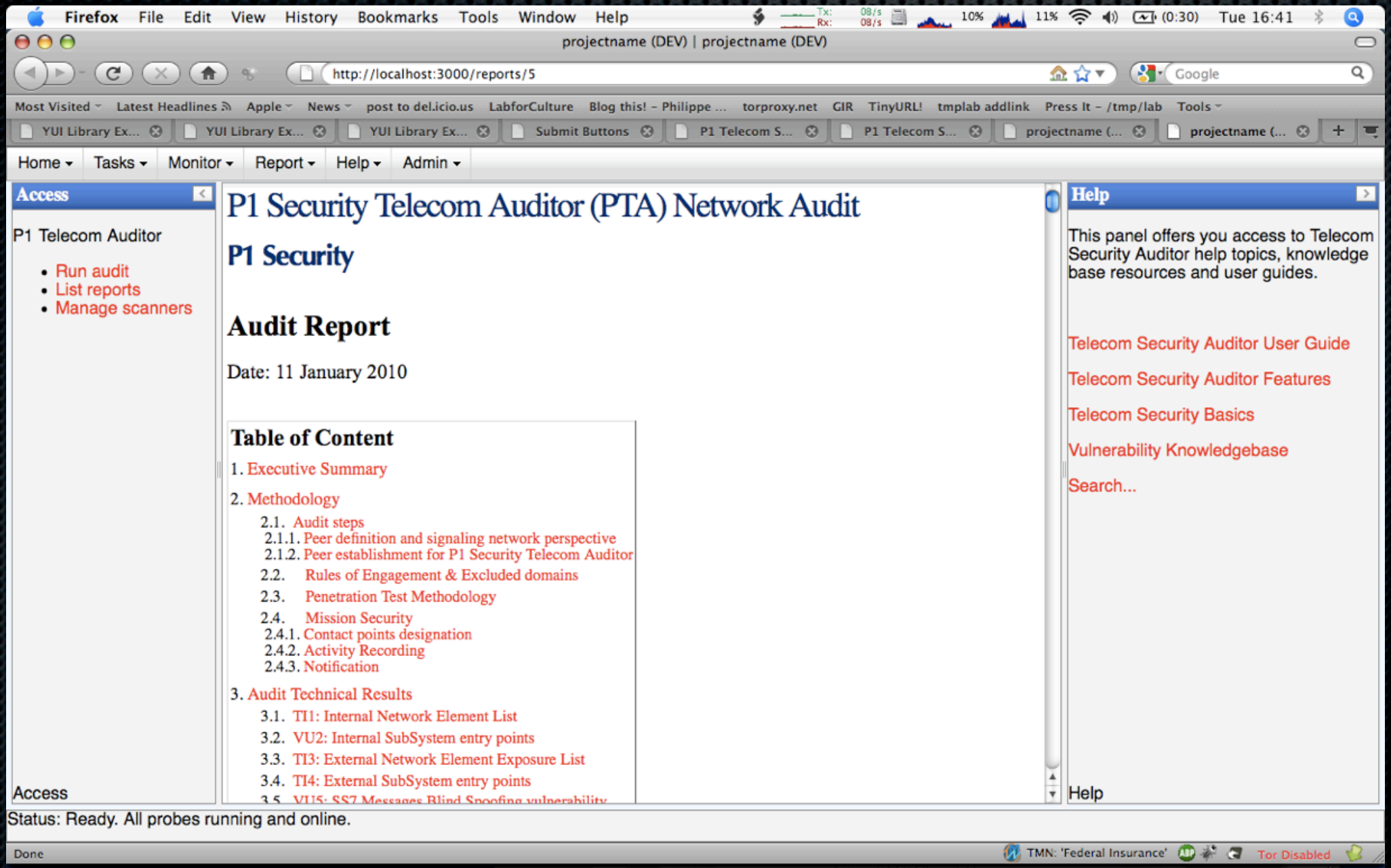
Report

- Generated with graphs, detailed analysis and raw data from the probe.
- Direct expert contact for assistance and expertise.
- Reference to knowledge base of past and current attacks on telecom networks.
- KB Constantly updated.

http://www.p1security.com/

PTA Report

P1 Security
Priority One Security



http://www.p1security.com/

P1 Security
Priority One Security

Who?

- Established management team
  - Avg of 15 year of industry background, both Security and Telecom.
  - Successful Entrepreneurs (Qualys, INTRINsec, TSTF)
- Start-up launched in January 2009
  - Already established references in Europe and Asia
  - Financial backing from private investors

http://www.p1security.com/

Questions

P1 Security
Priority One Security

Any question, ask sales@p1sec.com